NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Cases: 79204X, 79825A
and 85643B
1 July 2019

JASON LEOPOLD
C/O JOSEPH C. KELLY
1712 EYE STREET, NW SUITE 915
WASHINGTON DC 20006

Dear Mr. Leopold:

This letter is in response to your Freedom of Information Act (FOIA) request dated 20 September 2014 for "disclosure from the National Security Agency Office of Inspector General a copy of the concluding document (report of investigation, final report, closing memo, referral letter) concerning investigations closed in calendar year 2013 and 2014 concerning misconduct, actual or alleged." You advised on 26 September 2014 that you wished to amend your request to "a copy of the concluding document (report of investigation, final report, closing memo, referral letter) concerning investigations closed in calendar year 2013 and 2014 concerning ONLY findings of misconduct." As stated in our initial letter, dated 23 September 2014, your request was assigned Case Number 79204.

Please note that this letter also provides interim responses to the following 2 additional and related Freedom of Information Act (FOIA) requests that are covered by the same civil complaint (1:16-cv-02258):

- FOIA request dated 30 November 2014 for "...disclosure from the National Security Agency Office of the Inspector General of copies of Semi-Annual Reports for the past 11 years." As stated in our initial response letter to this request, dated 2 December 2014, this request was assigned Case Number 79825.

- FOIA request dated 6 October 2016 for "...disclosure from the National Security Agency Office of Inspector General a copy of the concluding document (report of investigation, final report, closing memo, referral letter) concerning all investigations conducted and closed in calendar years 2015 and 2016 thus far concerning any and all misconduct, actual or alleged." As stated in our initial letter, dated 13 October 2016, this request was assigned Case Number 85643.

Your requests are being processed under the FOIA. We processed 22 documents totaling 406 pages for this release and 402 pages are enclosed.

FOIA Cases: 79204X, 79825A
and 85643B

We processed 5 documents totaling 176 pages for this release from case 79204. Three documents (172 pages) are enclosed. The remaining two documents (4 pages) were determined to be non-responsive to your request:

- Doc ID 6672215, pages NSA 08546 - 08586
- Doc ID 6672216, pages NSA 08587 - 08597
- Doc ID 6672264, pages NSA 08598 - 08717

We processed 16 documents totaling 221 pages for this release from case 79825 and they are enclosed.

- Doc ID 6672178, pages NSA 08727 - 08735
- Doc ID 6672179, pages NSA 08736 - 08746
- Doc ID 6672180, pages NSA 08747 - 08757
- Doc ID 6672181, pages NSA 08758 - 08772
- Doc ID 6672182, pages NSA 08773 - 08783
- Doc ID 6672185, pages NSA 08784 - 08796
- Doc ID 6672186, pages NSA 08797 - 08807
- Doc ID 6672187, pages NSA 08808 - 08817
- Doc ID 6672188, pages NSA 08818 - 08822
- Doc ID 6672189, pages NSA 08823 - 08830
- Doc ID 6672227, pages NSA 08831 - 08862
- Doc ID 6672265, pages NSA 08863 - 08892
- Doc ID 6672229, pages NSA 08893 - 08902
- Doc ID 6672230, pages NSA 08903 - 08909
- Doc ID 6672231, pages NSA 08910 - 08919
- Doc ID 6672232, pages NSA 08920 - 08947

We processed 1 document totaling 9 pages for this release from case 85643 and it is enclosed.

- Doc ID 6672217, pages NSA 08718-08726

Certain information has been deleted from the enclosures, as explained below.

Some of the information deleted from the documents was found to be currently and properly classified in accordance with Executive Order 13526. This information meets the criteria for classification as set forth in subparagraph (c) of Section 1.4 and remains classified TOP SECRET and SECRET and CONFIDENTIAL as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause damage to the national security, to include exceptionally grave or serious damage. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA, 5 U.S.C. Section 552(b)(1).

This Agency is authorized by various statutes to protect certain information concerning its activities as well as names of its employees. Accordingly, those

portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 50 U.S. Code 3024(i) and Section 6, Public Law 86-36 (50 U.S. Code 3605). We have determined that such information exists in these documents and we have redacted it accordingly.

Some of the information has been redacted from the enclosures pursuant to the fifth exemption of the FOIA. This exemption applies to inter-agency or intra-agency memoranda or letters that would not be available by law to a party other than an agency in litigation with the agency, protecting information that is normally privileged in the civil discovery context, such as information that is part of a predecisional deliberative process.

Personal information regarding individuals has been deleted from the enclosures in accordance with the sixth exemption of the FOIA, 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

The seventh exemption of the FOIA protects from disclosure records or information compiled for law enforcement purposes. This includes information that, if released, could interfere with enforcement proceedings, could cause an unwarranted invasion of personal privacy, or would reveal law enforcement techniques procedures. The information withheld under (b)(7)(E) from the enclosures, meets the threshold requirements for withholding under exemption 7 of the FOIA.

Finally, some information has been redacted pursuant to the IG Act of 1978, Sec 7(b), P.L. 95-452, which protects the confidentiality of employee complaints to the IG.

Please be advised that we continue to work on your requests, and the review of additional documents responsive to your requests continues.

Sincerely,

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

~~SECRET//X1~~

OFFICE OF THE INSPECTOR GENERAL

NATIONAL SECURITY AGENCY/

CENTRAL SECURITY SERVICE

(U) SEMIANNUAL REPORT FOR THE PERIOD

1 APRIL 2004 – 30 SEPTEMBER 2004

DERIVED FROM: JSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1~~

~~SECRET//X1~~

~~SECRET//X1~~

(b) (3)-P.L. 86-36

(U) SEMIANNUAL REPORT TO THE CONGRESS

For the Period April 1, 2004 Through September 30, 2004

(U) **Selected System Engineering Contracts**; NSA/CSS IG; ST-04-0009; 21 May 2004

Summary. (U//~~FOUO~~) Our review summarized the results of our analyses of two system engineering contracts identified in a recent report as warranting further review. The contracts with [redacted] and [redacted] had indications of questionable cost growth, continuing lack of competition, and failure to perform market research. The current review found that the [redacted] contract needs formal task orders, and the [redacted] contract missed opportunities for competition. We also noted an emerging issue: mergers and acquisitions within its contractor base make the Agency vulnerable to potential conflicts of interest among its vendors. The Contracting Officer and [redacted] now have a formal mitigation plan to resolve this concern.

Management Action. (U) Management concurred with our recommendation and is adding the proper task order clauses to the [redacted] contract. For the [redacted] contract, the OIG did not make a recommendation since the contract ended in June 2004 and the benefit would be minimal.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Other (Acquisition Management)

(U) **Restaurant and Civilian Welfare Funds**; NSA/CSS IG; AU-04-0014; 28 May 2004

Summary. (U//~~FOUO~~) NSA's Restaurant Fund and Civilian Welfare Fund CWF) are DoD revenue producing nonappropriated fund instrumentalites (NAFIs) that operate under Army and NSA/CSS regulations for morale and welfare purposes. The financial statements of the two NAFIs were audited by an outside audit firm, which issued unqualified opinions. The external audit for FY2003 found that drug store management and accountability improved significantly after implementation of recommendations made in our oversight review of the FY2002 audit. The compliance audit of the Flying Activity (conducted at our recommendation in last year's oversight audit of the CWF) identified four safety areas that need improvement: standard operating procedures, pilot qualification cards, clearing authority, and refueling away from the Flying Activity.

Management Action. (U) We endorsed the improvements recommended by the safety inspectors; management is acting on all of them.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Financial Management

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1~~

~~SECRET//X1~~

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) NSA/CSS IG;

Summary. (~~S~~) The OIG visited all locations in September 2003 and found that has been very effective in its primary responsibility— Nevertheless, the dilute effectiveness and create oversight and morale problems, especially among the military. Insufficient oversight, guidance, and support from NSA HQ contributed to many of the deficiencies noted during our inspection.

Management Action. (U) Management is taking corrective action on all recommendations.

Overall Report Classification. (U) TOP SECRET//COMINT/X1

Category. (U) Joint Warfighting and Readiness

(U) **Contract Accountability Investigation;** NSA/CSS IG; IV-04-0001; 06 July 2004

Summary. (U~~//FOUO~~) This investigation was a follow-on review to a FY2003 Special Study that found significant irregularities with the Agency's novation and administration of a Systems Engineering and Technical Assistance (SETA) contract. The supplemental investigation determined: 1) that the Government's involvement in the novation of the SETA contract was consistent with the Federal Acquisition Regulation, 2) that the Government's past performance assessment was skewed by a mistaken understanding of fact, however, correction of this error would not have altered the Government's ultimate conclusion regarding one contractor's suitability for the novation, and 3) that the Contracting Officer and the former Chief of NSA/CSS SIGINT Programs were responsible for the contracting deficiencies with the SETA contract.

Overall Report Classification. (U) CONFIDENTIAL//X1

Category. (U) Other (Acquisition Management)

(U) **Office of NSA/CSS Representative, Joint Forces Command**; NSA/CSS IG; IN-04-0004; 30 July 2004

Summary. (U~~//FOUO~~) Our inspection found that the NSA/CSS Representative, Joint Forces Command (NCR JFCOM) is not closely aligned with the new Command's mission, which is focused on joint concept development and experimentation and has no geographic area of responsibility. Effective representation at JFCOM is important because the Command is the birthplace of short- and long-term changes to the nation's military and its warfighting doctrine. We found the NCR not well positioned to do this because it lacks strategic guidance from HQ and is not accredited to the Command level. Vestiges of a SIGINT support mission waste Agency resources, despite several proposals from the NCR to reduce staff. The Information Assurance Directorate (IAD), on the other hand, is managing a growing portfolio of initiatives with JFCOM.

Management Action. (U) Management concurred with all but one recommendation and has either developed plans to resolve them or already implemented appropriate actions.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Joint Warfighting and Readiness

(U~~//FOUO~~) **Compliance with the Federal Information Security Management Act (FISMA) at NSA/CSS**; NSA/CSS IG; AU-04-0013; 6 August 2004

Summary. ~~(C)~~ The audit assessed the progress by the NSA/CSS Chief Information Officer in specific aspects of Information Assurance since last year's report on compliance with FISMA. Our audit found that NSA continues to make positive strides in improving the security posture of its networks and systems. The Defense-in-Depth approach—focused on people, operations, and technology—is starting to come together, but much remains to be done.

Management Action. (U~~//FOUO~~) Since last year's report, NSA management reduced the number of systems operating without C&A, established Plans of Action and Milestones to monitor the progress of efforts to correct security weaknesses, improved information technology (IT) security training, and established an Agency-wide Operations Security program. Furthermore, management took the first step to establish a verifiable IT system inventory and improve the IT investment management process.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Information Technology Management

(b) (1)
(b) (3)-P.L. 86-36

(U~~//FOUO~~) **Collecting Communications of a U.S. Person Abroad Without Attorney General Authorization**; NSA/CSS IG; ST-04-0016; 10 August 2004

Summary. ~~(C)~~ the Signals Intelligence Directorate (SID) targeted the communications of a U.S. person located abroad without the required Attorney General authorization. While conducting our inquiry into this mishap, we encountered strong indications of shortcomings in the control environment that allowed this incident to occur After interviewing officials from SID's Analysis and Production Directorate, the SID Office of Oversight and Compliance, and the NSA Office of General Counsel, we identified systemic problems that point to the lack of key elements that are critical to creating a strong control environment for this high-risk activity, including written guidance containing clearly defined roles and responsibilities for all involved in the process, defined policies and procedures, and tailored training in the process for those who handle special authorizations.

Management Action. (U) SID concurred with most of our recommendation and is taking appropriate corrective action.

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

Overall Report Classification. (U) SECRET//COMINT//X1

(b) (3)-P.L. 86-36 **Category.** (U) Other (Intelligence Oversight)

(U//~~FOUO~~) NSA/CSS IG; INSCOM IG; AIA IG; NSG IG;

Summary. ~~(C)~~ A joint inspection of by a team from the Service Cryptologic Elements and NSA/CSS found problems that have a direct impact on the site's effectiveness. The most significant issues for management to address include:

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//X1

Category. (U) Joint Warfighting and Readiness

(U) **GROUNDBREAKER Contract Costs** ; NSA/CSS IG; ST-04-0021; 13 September 2004

Summary. (U~~//FOUO~~) In September 2001, the GROUNDBREAKER (GB) Program Office awarded Eagle Alliance (EA) an $11.2 million Delivery Order to implement the special modernization provision in clause H.46 of the basic contract. Initially, EA proposed immediate replacement of 17,000 desktops within 1 year. Our review of a previous audit's recommendation found that by December 2002, almost 15 months after contract award, only 7,000 desktops had been purchased, far short of the 17,000 described in EA's modernization proposal. Deficiencies in the contract terms of the Delivery Order made it impossible to determine how the $11.2 million was spent or to track any equipment purchased with the money.

Management Action. (U) After reviewing the contractor's records, we recommended closing the recommendation in the audit followup system; however, we are considering additional oversight of the GB contract in FY2005.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Other (Acquisition Management)

~~(C)~~ **Disbursing Account at** NSA/CSS IG;

Summary. ~~(C)~~ Accounting and Financial Services (DF2) maintains a cash account at to pay for certain goods and services;

(b) (1)
(b) (3)-P.L. 86-36

[redacted] At the request of the Chief, Accounting and Financial Services, the OIG audited the account to resolve an apparent $5900 discrepancy and assess the implementation of prior OIG recommendations to improve cash management at the site. We found a cash shortage of about $2100, due in large measure to the site's failure to implement prior OIG recommendations. We also found that the site was holding excess amounts of cash—in some cases more than the disbursing agent is authorized to hold—which creates unnecessary risk and makes it harder to balance the account. The site bypassed controls to make $3100 in questionable payments, apparently authorized by [redacted] and not subsequently challenged by DF2.

Management Action. (U) Management agreed to report the cash shortage to the Defense Finance and Accounting Service to determine pecuniary liability. Management is also in the process of reducing the excess cash at the site. Finally, controls have been implemented to avoid making questionable payments.

Overall Report Classification. (U) CONFIDENTIAL

Category. (U) Financial Management

(U) **Special Processing Laboratory**; NSA/CSS IG; AU-04-0006; 13 September 2004

Summary. (U//~~FOUO~~) The Special Processing Laboratory (SPL) has produced classified microelectronic chips for NSA and other government organizations since 1991. However, when rapid advances in the industry left the SPL lagging from a technological standpoint, the Director, NSA decided to close the SPL by FY2006 and replace the capability with a commercial source—a Trusted Foundry Access (TFA). Our audit determined that the Agency needs a formal plan to transition a critical DoD program to the TFA. Another concern was payment of a 50-percent salary-based retention bonus for all SPL personnel, including those not affected by the closure. We also found that the DoD organizations that sent NSA about [redacted] to fund their portion of the FY2004 TFA contract [redacted] to utilize the contract. (b) (3)-P.L. 86-36

Management Action. (U//~~FOUO~~) The IAD is now developing a transition plan. We accepted IAD's proposal to exclude [redacted] SPL employees from the retention plan for a cost avoidance of about [redacted] Regarding the lack of [redacted] NSA and DoD have now formed an Integrated Process Team to work this problem.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Information Technology Management

(U//~~FOUO~~) **Management of Activities Under the Foreign Intelligence Surveillance Act (FISA) of 1978**; NSA/CSS IG; ST-03-0008; 27 September 2004

Summary. ~~(C)~~ Our review of NSA's management of electronic surveillance activities conducted under the FISA of 1978 found that those activities generally ensure that the rights of U.S. persons are protected. However, the Agency's internal management controls for those activities make the process confusing and unduly dependent on the unwritten knowledge of a few people. Management needs to improve controls over the FISA process

to include (1) written guidance that spells out authorities, roles, and responsibilities; (2) standard operating procedures with step-by-step instructions; (3) tailored training on FISA operations; and (4) metrics to gauge the efficacy of the process.

Management Action. (U~~//FOUO~~) Management has agreed to define the pertinent authorities and responsibilities by October 2004. The other control elements—formal procedures, tailored training, and metrics—will be in place by December 2005.

Overall Report Classification. (U) TOP SECRET//COMINT//NOFORN//X1

Category. (U) Other (Intelligence Oversight)

(b) (1)
(b) (3)-P.L. 86-36

(U) **Menwith Hill Station**; NSA/CSS IG; INSCOM IG; AIA IG; NSG IG; JT-04-0003; 30 September 2004

Summary. ~~(C)~~ Since the 2002 joint inspection of Menwith Hill Station (MHS), site leadership and NSA HQ have made great strides in correcting longstanding infrastructure problems, improving the quality of life for all assignees, and transitioning cryptologic host responsibilities to the Air Force. The joint inspection team found that MHS has demonstrated exceptional mission successes, but the explosion in target technology exceeds the site's capacity to process and store data, while sustained tasking leaves few – if any- resources for new mission development. The joint team noted other areas that require close and continued attention from MHS and NSA HQ : 1) jointly integrating and synchronizing operations and support [redacted] and; 2) directing the revitalization of major interdependent systems.

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//COMINT//TK//REL TO USA and GBR//X1

Category. (U) Joint Warfighting and Readiness

~~(C)~~ [redacted] NSA/CSS IG, INSCOM IG, DAIG; [redacted]

Summary. ~~(S)~~ A team from the Army Intelligence and Security Command (INSCOM), NSA, and Department of the Army Inspectors General (DAIG) conducted an inspection of the [redacted]

Management Action. (U) Management is taking appropriate corrective action.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

Overall Report Classification. (U) SECRET//COMINT//X1

Category. (U) Joint Warfighting and Readiness

(U) **Corporate Level Functions;**NSA/CSS IG;(Numerous Special Study Control Numbers); 30 September 2004

Introduction. (U) During the October 2000 Senior Day briefing and in subsequent DIRgrams, the Director, NSA (DIRNSA) called for the centralization of mission-enabling functions. His goals were to dedicate SID and IAD resources to mission accomplishment and to eliminate duplication of effort throughout the enterprise. In April 2003, DIRNSA asked the OIG to determine how well the Agency has met his charge to consolidate corporate-level functions under centralized corporate sponsors. Over the past year, the OIG completed reviews of the following functions:

Human Resource Services
Protocol
Legislative Affairs
Acquisition and Finance
Information Technology Infrastructure Services
Installations and Logistics
Security
Policy
Education and Training

Summary. (U) During our reviews, we found differing degrees of centralization. We made recommendations to management and management is taking appropriate action.

Overall Report Classifications. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY and CONFIDENTIAL//X1

Category. (U) Human Capital (for all Corporate-Level Function Reports)

(U) **False Claims;** NSA/CSS IG, IV-04-0010, May 2004

Summary. (U) An Agency employee deliberately submitted a fraudulent timesheet reflecting duty time, as well as a fraudulent travel voucher requesting reimbursement for travel expenses that were not incurred in connection with the employee's official duties. Disciplinary action is pending, and the case was referred to the Department of Justice for possible prosecution under federal false claims statutes, 18 U.S.C. § 287 and 18 U.S.C. § 1001.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Other (Fraud)

(U) **Time and Attendance Abuses**; IV-04-0035 (10 May 04), IV-04-0038 (9 September 04), IV-04-0041 (27 September 04), IV-04-0048 (8 September 04), IV-04-0050 (17 September 04), IV-04-0055 (24 September 04), IV-04-0062 (30 September 04)

Summary. (U~~//FOUO~~) The OIG substantiated seven Time and Attendance Abuse allegations, wherein employees claimed hours in excess of those they were determined to have actually worked. In the aggregate, these cases will result in the recoupment of almost $30,000 in funds paid to employees for hours falsely claimed. Several of these cases were referred to the U.S. Department of Justice for possible prosecution of violations of 18 U.S.C. § 287 and 18 U.S.C. § 1001.

Overall Report Classifications. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

Category. (U) Other (Fraud)

(U) **Misuse of Resources**; NSA/CSS IG, IV-04-0020, June 2004

Summary. (U~~//FOUO~~) The OIG substantiated an allegation that a planned TDY for training was a waste of government resources. The OIG determined that identical training could be obtained locally at a greatly reduced rate. Based upon the OIG's recommendation, Agency management cancelled the planned training, saving the Government over $37,000.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Other (Misuse of Resources)

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) *For the Period October 1, 2005 Through March 31, 2006*

(b) (3)-P.L. 86-36

(U) **Controls on Laptop Computers;** NSA/CSS IG; ST-05-0015; 25 October 2005

(U//~~FOUO~~) **Summary.** After conducting many investigations of missing laptop computers, the Compromise and Computer Forensics Office asked the NSA OIG to review the Agency's inventory processes and determine whether the Agency has adequate controls to track and account for laptop computers. Over the past 3 years, the Compromise and Computer Forensics Office conducted [redacted] investigations of missing laptops but was unable to locate [redacted] ([redacted] classified, [redacted] of unknown classification, and [redacted] unclassified) of the [redacted] laptops. Such losses, while financially immaterial, raise counterintelligence concerns.

(U//~~FOUO~~) **Management Action**. To address the root cause of the losses—the lack of hand receipts for laptops—the Security, Logistics, and OIG organizations are strengthening the enforcement of laptop controls, including penalties for personnel who do not comply with the hand receipt requirement and managers who fail to enforce it. The three organizations will meet every 90 days to discuss the enforcement of the hand receipt policy and ways to hold managers accountable

(U) **Overall Report Classification.** CONFIDENTIAL

(U) **Category.** Information Technology Management

(U) [redacted] NSA/CSS IG; [redacted]

(U//~~FOUO~~) **Summary.** [redacted]

(U) **Management Action**. Management agreed to act on all our recommendations. However, Signals Intelligence Directorate and Information Technology Directorate are still working out the appropriate division of effort and responsibilities for managing and optimizing data flow.

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~20291123~~

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(U) **Misuse of Government Resources**; NSA/CSS IG; IV-05-0027; 17 November 2005

(U//~~FOUO~~) **Summary.** The OIG's Offices of Intelligence Oversight and Investigations conducted a joint inquiry into an allegation that an NSA/CSS employee violated applicable law and regulation by using Government property for unauthorized and unofficial purposes. We substantiated the misuse allegation and referred the matter to the NSA/CSS Office of the General Counsel, for consideration of referral to the DOJ.

(U) **Overall Report Classification.** TOP SECRET//COMINT

(U) **Category.** Other (Intelligence Oversight)

(U) **Contractor Performance Management and Evaluation of the GROUNDBREAKER Contract**; NSA/CSS IG; AU-05-0002; 16 December 2005

(U//~~FOUO~~) **Summary.** This audit focused on improving the use of rewards and penalties to motivate the contractor to optimize performance. Our audit found that, although the modernization goal of May 2004 had slipped by 17 months, the contractor received $10.7 million out of a possible $20.9 million in award fees for modernization. In this case, award fees were not used in a way that motivated the contractor to meet a crucial performance goal. Additionally, millions of dollars in service credits (penalties for failure to deliver agreed-to services) that should have been credited to the Agency were not recorded as accounts receivable and reported on financial statements. This ultimately cost the Government $300,000 in finance or interest charges from July 2002 to March 2005.

(U) **Management Action.** After initially nonconcurring with our recommendation to improve modernization incentives, management revised its position and is developing new, more objective incentive criteria. Corrective actions are now under way or completed on all six recommendations.

(U) **Overall Report Classification.** CONFIDENTIAL

(U) **Category.** Acquisition Processes and Contract Management

(b)(3)-P.L. 86-36

(U) **Advisory Report on the Audit of the [redacted] Procurement and Associated Infrastructure Program**; NSA/CSS IG; [redacted]

(U//~~FOUO~~) **Summary.** The advisory report identified potential issues that surfaced during the survey phase of our audit of the [redacted] Procurement and Associated Infrastructure Program. We curtailed our survey after reviewing a zero-based review of Cryptanalysis Exploitation Services, which included [redacted] Our survey supported the conclusions of the zero-based review: lack of sustained funding threatens the [redacted] infrastructure; the physical facilities are inadequate; acquisition

(b)(3)-P.L. 86-36

practices are inconsistent; and there is insufficient mission assurance for [redacted] In addition, our survey indicated that the Portfolio Management Office lacked sufficient authority over program execution and resources.

(U) **Management Action.** Since the recommendations for [redacted] in the zero-based review are related to the indications noted during our audit survey, we will track completion in the OIG Followup system.

(U) **Overall Report Classification.** TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL/[redacted]

(U) **Category.** Acquisition Processes and Contract Management

(U) **Nuclear Command and Control (NC2) Program**; NSA/CSS IG; AU-04-010B; 23 January 2006

~~(S)~~ **Summary.** Our audit revealed that the [redacted] Board and management of the Nuclear Command and Control Program (NC2) [redacted]

(U) **Management Action.** Management agreed to act on all recommendations.

(U) **Overall Report Classification.** TOP SECRET//NOFORN

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) **Category.** Joint Warfighting and Readiness

(U) **Aerospace Data Facility**; NSA/CSS IG; INSCOM IG; NSG IG; AIA IG; JT-06-0001; 23 January 2006

~~(S)~~ **Summary.** The joint inspection found that the Aerospace Data Facility has [redacted]; 2) NSA HQ organizations have not provided policy, standards, or oversight of various efforts across the Extended Enterprise; and 3) the lack of a mission management tool hinders the site's ability to optimize its role in consolidated mission planning and execution.

(b)(1)
(b)(3)-P.L. 86-36

(U) **Management Action.** Management concurred with the recommendations and is taking appropriate corrective action.

(U) **Overall Report Classification.** TOP SECRET//COMINT/TALENT KEYHOLE//REL TO USA, AUS, GBR

(U) **Category.** Joint Warfighting and Readiness

(U//~~FOUO~~) **Red Team Targeting of the** [redacted] NSA/CSS IG; [redacted] (b) (3)-P.L. 86-36

(U//~~FOUO~~) **Summary.** The National Defense Authorization Act of Fiscal Year 2000 directs the National Counterintelligence Executive (NCIX) to submit an annual report to the Secretary of Energy and the Director of the Federal Bureau of Investigation on the security vulnerabilities of the computers of the DOE's national laboratories. [redacted]

[redacted]

(U//~~FOUO~~) **Management Action.** NSA management has amended the Red Team process and procedures to require, for each exercise, [redacted]

[redacted]

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Joint Warfighting and Readiness

(U) **Post-Accreditation Process for Information Technology Systems**; NSA/CSS IG; ST-05-0018; 16 February 2006

(U//~~FOUO~~) **Summary.** Our special study of the post-accreditation process for information technology systems sampled [redacted] systems that recently went through the accreditation process and were [redacted] of the systems were not operational and, [redacted]

[redacted]

(b) (3)-P.L. 86-36

(U) **Management Action.** The Information Assurance Directorate responded that it is working on a post-accreditation process that satisfies the recommendations of the OIG report.

(U) **Overall Report Classification.** TOP SECRET//NOFORN

(b) (1)
(b) (3)-P.L. 86-36

(U) **Category.** Information Technology Management

~~(C)~~ **SIGINT Activities** NSA/CSS IG, INSCOM IG; AIA IG;

~~(S)~~ **Summary.** A joint team of inspectors from the AIA, INSCOM, and NSA Inspectors General conducted an inspection of

(U) **Management Action.** The report makes ten recommendations to improve the effectiveness and efficiency of SIGINT operations. Most of these recommendations focus on the need to bring greater definition to the authorities, responsibilities and functions with respect to the operational roles of the SIGINT sites. Management concurred in all recommendations and corrective action is being taken.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(U) **"Persistent Cookies" on the NSA Public Website;** NSA/CSS IG; ST-06-0015; 21 March 2006

(~~U//FOUO~~) **Summary.** The OIG conducted an inquiry into the circumstances and implications of the Agency's usage of "persistent cookies" on its public website, NSA.gov. We concluded that, during a past system upgrade, a number of cookie properties were unintentionally reset, extending their expiration beyond the intended settings. As a result, the website was inadvertently using "persistent cookies" instead of the usual "session cookies." Once aware of the situation, the Agency immediately disabled the "persistent cookies" and restored the intended session length settings. Based upon our interviews, contacts, and reviews of databases and technical literature, we concluded the Agency's inadvertent "persistent cookies" did not collect user information or any personally identifiable information on visitors to the NSA.gov website.

(U//~~FOUO~~) **Management Action.** Corporate Communications Strategy Group personnel have begun documenting the programming code with comments where system changes could inadvertently enable different types of cookies. The Group intends to have comprehensive procedures written and implemented by July 2006, and has suspended any system upgrades until then.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other

(U//~~FOUO~~) **Special Study of Executive Level Management of Systems Development at NSA/CSS;** NSA/CSS IG; ST-05-0004; 22 March 2006

(U//~~FOUO~~) **Summary.** At the corporate level, NSA/CSS needs a formal, stable, unified methodology to enable its leadership team to wield effective oversight of key development programs. This is even more necessary as the Agency accelerates transformation efforts. The existing disparate approaches to program oversight in several Agency organizations should be unified into an overarching methodology under the leadership of one organization or individual. An OIG benchmarking study of two information-intensive organizations in the private sector and one major DoD development program supported the conclusion that until NSA/CSS adopts such a methodology, its leaders will not have the requisite degree of insight into all aspects of key enterprise initiatives. By the end of the study, it was clear that the Agency needs such a methodology to lead the work force successfully through the pervasive changes underway in its mission and core business.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Joint Warfighting and Readiness

(U//~~FOUO~~) **Interim Report on the Audit of NSA's Computer Security Incident Response;** NSA/CSS IG; AU-05-011A; 24 March 2006

~~(S)~~ **Summary.** During our audit of NSA's Computer Security Incident Response, the NSA/CSS Information Systems Incident Response Team (NISIRT) told us about a vulnerability created by default settings [redacted]

(U) **Management Action.** The Information Technology Directorate responded that it is working to secure current and future [redacted] which satisfies our recommendation.

(b)(1)
(b)(3)-P.L. 86-36

(U) **Overall Report Classification.** TOP SECRET//NOFORN

(U) **Category.** Information Technology Management

(U//~~FOUO~~) **Misuse of the Agency's Unclassified Network;** NSA/CSS IG; ST-05-0019; 28 March 2006

(U//~~FOUO~~) **Summary.** After expending considerable resources to address misuse of the Internet by Agency affiliates, the NSA/CSS Information Systems Incident Response Team (NISIRT) asked the OIG to review the adequacy of the Agency's policies regarding usage of NSA's unclassified network. We concluded that the Agency's current policies, the Computer Security Incident Report process and a new "Smart Filter" which will deny user access to inappropriate web sites are adequate tools for dealing with misuse. However, we also found that many affiliates are not aware of current policies, and that managers are not informed of misuse by their subordinates.

(U//~~FOUO~~) **Management Action.** Management agreed to implement annual training on Internet policies for affiliates, and NISIRT agreed to advise managers of policy violations so they can hold subordinates accountable.

(U) **Overall Report Classification.** CONFIDENTIAL//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Information Technology Management

(b) (3)-P.L. 86-36

(U//~~FOUO~~ **Dorsey Road Warehouse;** NSA/CSS IG;

~~(S)~~ **Summary.** While investigating a procurement matter involving computer equipment shipped to the Dorsey Road Warehouse (DRW) We undertook a special study to determine whether DRW

~~(S)~~ **Management Action.** In response to our findings, the Associate Directorate for Security and Counterintelligence and Associate Directorate for Installations and Logistics developed short- and long-term strategies These strategies addressed our concerns, and we will track implementation through our followup system. We consider implementation a high priority that should be funded as such.

(U) **Overall Report Classification.** SECRET

(b) (1)
(b) (3)-P.L. 86-36

(U) **Category.** (U) Infrastructure and Environment

(U) **False Labor Charges by an Agency Contractor;** NSA/CSS IG; IV-05-0031; December 2005

(U//~~FOUO~~) **Summary.** During a routine Security background check, suspicions surfaced about the accuracy of labor charges by an NSA/CSS contractor employee. An OIG investigation substantiated that, during a 22-month period, the contractor employee falsely billed 751 labor hours to an Agency contract, amounting to approximately $35,000 in false charges. The matter was referred to the DOJ for a prosecutive opinion, and the NSA/CSS Office of the General Counsel is seeking restitution from the involved company.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Acquisition Processes and Contract Management

(U) **Time and Attendance Investigations**; NSA/CSS IG; IV-05-0008 (10 Nov 2005); IV-05-0035 (4 Oct 2005); IV-06-0014 (10 Mar 2006); IV-06-0026 (24 Mar 2006); IV-06-0021 (30 Mar 2006)

(U//~~FOUO~~) **Summary.** The OIG substantiated five allegations of Time and Attendance abuse, wherein employees claimed hours in excess of those they were determined to have actually worked. In the aggregate, these cases will result in the recovery of approximately $44,000.00 in funds paid to employees for hours falsely claimed.

(U) **Overall Report Classifications.** UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

(U) **Category.** Other (Fraud)

(U) **Unauthorized Commitment of Government Funds and Intentional Falsifications;** NSA/CSS IG; IV-05-0015; March 2006

(U//~~FOUO~~) **Summary.** An NSA/CSS employee made an unauthorized commitment of Government funds by accepting approximately [redacted] equipment without a contract. The employee and an Agency contractor then attempted to conceal the unauthorized action by creating and back-dating a fictitious "Loan Agreement," and by providing the OIG with false testimony. The employee and contractor violated applicable Federal regulations and possibly Title 18, United States Code, Section 1001.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Acquisition Processes and Contract Management

(b) (3)-P.L. 86-36

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U) Completed from 1 October 2005 – 31 March 2006

(U//~~FOUO~~) **Advisory Report on Activities Associated with Expeditionary SIGINT Deployments to Hostile Areas**; NSA/CSS IG; ST-06-0001; 23 January 2006

(U//~~FOUO~~) **Summary.** A February 2005 after-action report raised serious concerns about the activities and processes associated with the deployment of NSA/CSS personnel to hostile areas. The issues were referred to the OIG, which conducted extensive research to determine if a formal review was needed. Based on interviews of [redacted] organizations involved in the deployment process and [redacted] returnees from hazardous area deployments, such as [redacted] we concluded that some aspects of the process, especially training by enabler organizations, have improved considerably over the last 2 years. Processes to ensure appropriate and timely candidate selection, pre-deployment mission training, IT support, and corporate resolution of issues raised in after-action reports need to be standardized and implemented across the Agency.

(U) **Management Action.** Corrective measures addressing the issues are already underway; as such, we do not plan to undertake a formal review at this time. However, the issues raised merit continued action and followup by Agency management. We plan to revisit these processes again in 1QFY07 to assess progress.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness [redacted] (b)(3)-P.L. 86-36

(U) Ongoing

(U//~~FOUO~~) ***Inspection of the Information Warfare Support Center***; NSA/CSS IG; IN-06-0001

~~(S)~~ **Background** The Information Warfare Support Center (IWSC) began operations in November 1994 in response to the need for SIGINT support to Information Operations (IO). IWSC's mission is to provide the combatant commander(s) with [redacted] related to counterterrorism. The primary objectives of this inspection include the following: a) determining whether the [redacted] is executing its current missions and functions in an efficient and effective manner and in accordance with its charter, identifying any impediments to mission accomplishment; b) determining whether [redacted] personnel comply

[redacted] (b)(1) (b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

with Internal Management Controls and other Agency regulations and policies governing personnel and organizational management; and c) assessing how well [redacted] shares information with internal and external customers.

(U) **Inspection of SID's Chemical, Biological, Radiological, Nuclear Mission**; NSA/CSS IG; IN-06-0002

~~(S)~~ **Background.** Chemical, Biological, Radiological, and Nuclear (CBRN) terrorism is one of the most menacing threats to U.S. security, and from a Signals Intelligence (SIGINT) perspective [redacted] The inspection is evaluating CBRN mission performance, including examining the execution of CBRN as a transnational target, assessing the impact of Mission Build-Out, and reviewing any funding or human resource issues.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) **Special Studies of Presidentially-authorized Program**; NSA/CSS IG

(U~~//FOUO~~) **Background:** The OIG is performing continual audits of NSA's Presidentially-authorized counterterrorism program. The overall objectives are to determine whether there are appropriate policies and procedures in place for activities under the program consistent with the terms of the Presidential Authorization; to evaluate their efficiency and effectiveness in mitigating any high-risk activities associated with the program; and to identify any impediments to satisfying the requirements of the Presidential Authorization.

(U) Planned

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U~~//FOUO~~) **Inspection of the Geospatial Exploitation Office**; NSA/CSS IG; IN-06-0005

~~(S)~~ **Background** The Geospatial Exploitation Office (GEO) began operations in [redacted] The primary objective will be to assess GEO's mission effectiveness and their ability to satisfy requirements and information needs levied on the organization. The inspection will determine whether the current organization's missions and functions are being properly executed in an efficient and effective manner; whether missions and functions are accurately portrayed and being accomplished; establish whether missions performed are appropriately placed within the product line; and will identify any impediments, which hinder the efficient and effective execution of their missions and functions.

(b)(1)
(b)(3)-P.L. 86-36

~~(S)~~ **Office of Middle East and North Africa**; NSA/CSS IG; IN-06-0006

~~(S)~~ **Background.** The mission of the Signals Intelligence Directorate 's Deputy Directorate for Analysis and Production includes the countries located in the Middle East and North Africa (MENA). The Office of MENA [redacted] Our inspection will evaluate the mission effectiveness of MENA and its ability to satisfy requirements and information needs levied on the organization.

~~(S)~~ [redacted] **Regional Review**; NSA/CSS IG [redacted]

~~(S)~~ **Background.** The OIG plans to conduct a regional review of [redacted] sites that are focused on [redacted] including support to counterterrorism. Our review will assess site operations, compliance with intelligence oversight requirements, [redacted] and local support activities.

(U) **Followup Review of Access to SIGINT Databases**; NSA/CSS IG; ST-06-0003

~~(S)~~ **Backgound.** Information sharing and data access continue to be major priorities across the Intelligence Community (IC). To jumpstart the information-sharing concept, several efforts were initiated, most notably the efforts to provide [redacted]

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~SECRET//REL TO USA, FVEY~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

(b) (3)-P.L. 86-36

(U) *For the Period October 1, 2007 Through March 31, 2008*

(U//~~FOUO~~) ; NSA/CSS IG;

(~~S//REL~~) **Summary.** During September and October 2007, the NSA/CSS Office of the Inspector General (OIG) conducted a special inquiry into an allegation that We found no violations of NSA's legal compliance and minimization procedures and issued no formal recommendation, but we observed that additional oversight familiarization training was needed.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, FVEY

(U) **Category.** Other (Operational Authorities)

(U) **Contract Warehouse Operations;** NSA/CSS IG; AU-07-0019; 14 November 2007

(~~C//REL~~) **Summary.** In support of the Information Technology Directorate (ITD), the Agency contracts for warehouse space to store more than pieces of information technology equipment and parts valued at These warehouse services cost the Agency about annually. We performed this audit to evaluate the effectiveness and efficiency of the storage facilities contract to satisfy the Agency's requirements and needs. Our audit found that the Contracting Officer Representative must develop and implement a sampling plan to verify the accuracy of the contractor's inventory records. Additionally, the Property Acquisition Support Office must tag all of the ITD's pilferable items destined for the contract warehouse and account for them in the Defense Property Accountability System as required by NSA/CSS *Financial Management Manual 7-2*. Finally, some deliveries are

(U) **Management Action.** Management concurred with the recommendations.

(U) **Overall Report Classification.** SECRET//NOFORN

(U) **Category.** Acquisition Processes and Contract Management

(U) **Agency's Streaming Media Capability;** NSA/CSS IG; AU-07-0020; 4 December 2007

(U//~~FOUO~~) **Summary.** In April and July 2007, the OIG received similar hotline complaints about organizations duplicating streaming media and web services to the

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

Agency. In a 2006 Inspection Report, OIG found the same problem—Agency organizations use their own personnel or pay contractors to provide multimedia services instead of using the corporate authority (Office of Multimedia Solutions). Although the [redacted] has a legitimate role in providing operational streaming media in support of Signals Intelligence analysts, it has, on limited occasions, duplicated services offered by the Office of Multimedia Solutions. Although this office is responsible for web design and development of organizational and project websites on the NSA intranet as required by NSA/CSS Policy 10-7, other organizations are performing identical services. Duplication occurs because responsibilities of the Office of Multimedia Solutions and other Agency organizations are not clearly defined.

(U) **Management Action.** The Chief of Staff and Technology Directorate concurred with all recommendations and have initiated corrective actions.

(U) **Overall Report Classification.** SECRET//REL TO USA, FVEY

(U) **Category.** Other (Information Technology) [redacted]

(U) **Laptop and Other Portable Computing Devices Accountability**; NSA/CSS IG; AU-07-0005; 4 December 2007

(U//~~FOUO~~) **Summary.** Since 2000, the Agency has focused on improving its accounting of portable computing devices (PCDs), such as laptop computers. Nonetheless, as of 29 June 2007 the Agency had not accounted for some [redacted] of the more than [redacted] PCDs in use at NSA over the period 2000-2007. Our audit found that, although improvements had been made in tracking and identifying PCDs at the Agency, the audit trail for PCDs was inefficient and, in some cases, non-existent, especially for the hand-receipt process for Agency-owned and contractor-provided PCDs. Despite adequate accountability procedures for incoming property through Central Receiving, Agency personnel could bypass that process. Consequently, PCDs were brought into the Agency and not properly accounted for in property records. Missing or unaccounted for PCDs were not always reported as soon as they were known to be lost. Meaningful investigations cannot be conducted when missing PCDs, [redacted] are not reported quickly.

(U//~~FOUO~~) **Management Action.** After issuance of the audit report in December 2007, the Director, NSA/CSS tasked the Agency's Senior Leadership Team (SLT) to address the persistent problem of unaccounted-for laptops within the Agency. From December 2007 until February 2008, under the leadership of the Chief of Staff, the Agency conducted an exhaustive search for laptops, significantly reducing the number of unaccounted-for laptops identified in our audit report; developed a new Standard Operating Procedure (SOP) for laptop controls and accountability; approved technical measures to protect data on PCDs and track laptops; and withheld performance bonuses for 2007 for most SLT members until the search had been concluded and the SOP developed.

(U//~~FOUO~~) In February 2008, the SLT directed a number of actions, including

(b) (3)-P.L. 86-36

the preparation of a written report on these issues. On 7 March 2008, the Deputy Chief of Staff submitted the required report to the SLT. It included a history of the laptop accountability issue at NSA since 2002, results of the recent intensive efforts, and major actions that lie ahead. Attachments to the report included detailed results of the search and the new accountability procedures prepared by the OIG, Office of General Counsel, Directorate of Security, and Directorate of Installations and Logistics.

(U) Overall, the Agency is seriously addressing the issue of laptop accountability and is well on its way to establishing a systemic solution to this challenge, incorporating procedures that could be considered for adoption elsewhere in the Intelligence Community.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(b) (1)
(b) (3)-P.L. 86-36

(U) **Category.** Other (Information Technology)

(~~S//REL~~) NSA/CSS IG; (both reports)

(~~S//REL~~) **Summary.** We visited two sites selected on the basis of risk, location, and reported oversight issues. Our reviews assessed site operations, local customer support, and compliance with intelligence oversight requirements and instructions. At each site, we found some discrepancies between policy and the execution of Emergency Destruction Exercises. At one site, support to law enforcement was not fully coordinated.

(U) **Management Action.** management at the sites advised HQ that all employees had participated in Emergency Destruction Exercises after receiving clarification on procedures. Employees at one site have been reminded of the requirements of The other site will have a comprehensive environmental survey performed in 2008, and has confirmed receipt of a secure telephone.

(U) **Overall Report Classifications.** TOP SECRET//COMINT//NOFORN (both reports)

(U) **Category.** Joint Warfighting and Readiness

(b) (1)
(b) (3)-P.L. 86-36

(U) **Inquiry From Congress Concerning Possible USSID SP0018 Violations**; NSA/CSS IG; ST-08-0017; 17 December 2007

(U) **Summary.** In response to a request from the office of U.S. Senator Leahy of Vermont, we reviewed allegations of improper intelligence activities and violations of SIGINT authorities made by a citizen of Vermont, who had been a U.S. Army Reservist deployed to Fort Gordon, Georgia, in October 2001. We were unable to substantiate the allegations since the Reservist had never been assigned to NSA and had not performed an NSA mission while deployed.

(U) **Management Action.** We provided our findings for further action to the

Assistant to The Secretary Of Defense (Intelligence Oversight) and the Inspectors General of the Department of Defense, Department of the Army, and the U.S. Army Intelligence and Security Command.

(U) **Overall Report Classification.** SECRET//COMINT//NOFORN

(U) **Category.** Other (Operational Authorities)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) **Joint Inspection of NSA/CSS Europe;** NSA/CSS IG; AFISRA IG; INSCOM IG, NNWC IG; JT-07-0004; 18 December 2007

(~~C//REL~~) **Summary.** The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency, Naval Network Warfare Command, Intelligence and Security Command, and NSA conducted a joint inspection at Stuttgart [redacted] Germany, in September 2007. For at least two years, NSA/CSS Europe leadership (NCEUR) has focused on [redacted] The SIGINT Director has supported these initiatives and has adopted certain authorities. Under NSA/CSS Policy 1-3 on governance, the NCEUR transformation must be appropriately codified. Each Senior Functional Authority responsible for mission and enabling functions must formally delegate authorities in its management directives and allocate appropriate manpower and financial resources. Inspectors found many in the NCEUR workforce were unaware of or confused about their own and other organizational roles in the ongoing transformation. More effective communication of the NCEUR vision and the Director's intent is a major challenge. Joint inspection activities uncovered several areas where additional management oversight is needed, including safety, logistics, property accountability, training, Intelligence Oversight and cover travel.

(U) **Management Action.** Management concurred with all recommendations and corrective actions are underway.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, FVEY

(U) **Category.** Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

(~~C//REL~~) **Retention of Domestic Communications Collected Under FISA Surveillances;** NSA/CSS IG; ST-06-0007; 21 December 2007

(~~C//REL~~) **Summary.** While conducting collection operations authorized under the Foreign Intelligence Surveillance Act (FISA) of 1978, as amended, NSA might incidentally collect domestic communications subject to limitations. Our evaluation, conducted from September 2006 through August 2007, showed that: 1) although NSA collection systems and raw traffic databases can be programmed to facilitate compliance with retention procedures, some processing and retention procedures had not been programmed; 2) appropriate training on how data repository systems can improve analyst compliance with retention rules should diminish the unintentional override of these features; and 3) developing an automated dissemination system could lower NSA's risk of noncompliance.

(U) **Management Action.** Management concurred with the recommendations.

Corrective actions are underway on programming and training, and management is devising a plan to lower risks associated with dissemination.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Other (Operational Authorities)

(U//~~FOUO~~) NSA/CSS IG;

(~~S//REL~~) **Summary.** In FY2008, the OIG reported that . During the review, passage of the Protect America Act changed the overall authority under which surveillance directed at persons reasonably believed to be outside the United States could be conducted. That Act has now expired, but the conclusions of the OIG study are still valid. The OIG recommended changes in training and internal control procedures to avoid future collection incidents.

(U) **Management Action.** Management concurred with all recommendations and corrective actions are underway.

(U) **Overall Report Classification.** TOP SECRET//COMINT

(U) **Category.** Other (Operational Authorities)

(b) (1)
(b) (3)-P.L. 86-36

(U) **Inquiry Into Tasking Incidents in** NSA/CSS IG;

(~~S//REL~~) **Summary.** During August and September 2007, the OIG conducted a special inquiry into incidents that took place in limited period, but NSA could not verify whether The OIG recommended changes in internal control procedures to avoid future compromise of

(U) **Management Action.** The SIGINT Directorate concurred with the recommendations and has proposed plans to protect the data.

(U) **Overall Report Classification.** TOP SECRET//COMINT /NOFORN

(U) **Category.** Other (Operational Authorities)

(U) **Information Technology Enterprise Management System;** NSA/CSS IG; AU-06-0018; 21 December 2007

(~~S//REL~~) **Summary.** In FY2002, Congress recognized the need for an Information Technology Enterprise Management System (ITEMS) program at NSA. Although the Agency has been slow to implement an Enterprise Management System (EMS) that will monitor the health, status, and security of the Agency's Information Technology (IT) Infrastructure, ITEMS is currently regarded as a key program in the Agency's IT modernization effort. As of 30 June 2007, the estimated cost of the ITEMS program Our audit found that program requirements are not well defined

(b) (1)
(b) (3)-P.L. 86-36

because of inadequate stakeholder involvement, a weak governance process, and insufficient senior Agency management sponsorship. Without full funding and adequate staffing, ITEMS may not meet its goal of delivering a centralized EMS capability to NSA. As a result of recent budget cuts [redacted] Further, the program's small government staff creates the risk of inefficient program management and potentially puts too much reliance on contractor support for important program work and decision-making.

(U) **Management Action.** Management concurred with all recommendations, and corrective actions are underway.

(U) **Overall Report Classifications.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Joint Warfighting and Readiness

(b) (3)-P.L. 86-36

(U) **Quick Reaction Report — [redacted] Closeout**; NSA/CSS IG [redacted]

(~~C//REL~~) **Summary.** On 3 August 2007, the OIG received a complaint that alleged mismanagement of the [redacted] closeout. Our ongoing audit of the [redacted] Closeout disclosed a problem that warrants immediate attention by Agency leadership because valuable resources are being expended [redacted] The complaint specifically questioned [redacted] We found that the [redacted] had not conducted sufficient research to determine the most cost effective method for [redacted] This occurred because the Office was unaware that [redacted]

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Joint Warfighting and Readiness

(b) (1)
(b) (3)-P.L. 86-36

(U) **Follow-up Audit of the Special Study of Time Synchronization**; NSA/CSS IG; AU-07-0018; 23 January 2008

(U//~~FOUO~~) **Summary.** To accomplish its various missions, NSA must reliably affix accurate time-date stamps and, when available, geolocation information on all collected signals. However, NSA currently has no way to certify the accuracy of time-related information, even to the extent of accurately specifying the order of events. Key Agency organizations agree that synchronized time is crucial to the mission and must be established. To fix this long-standing Agency problem, the Time and Frequency Coordination Authority (TFCA) was established in May 2006. The objective of our audit

was to follow-up on the TFCA's progress to establish and implement an enterprise-wide time synchronization solution. Our follow-up audit found that, although TFCA has the authority, it does not have the organizational structure and resources necessary to direct and implement a time synchronization solution. The TFCA has not developed an acquisition plan, which would define user-timing requirements and include key performance goals, to eliminate the Agency's time synchronization deficiencies. Furthermore, the TFCA has not developed time standards and policies to ensure that consistent timing practices are applied across the Agency in support of the Signals Intelligence mission.

(U) **Management Action.** The Chief of Staff, Chief Technology Officer, and Senior Acquisition Executive agreed to implement corrective actions for the recommendations.

(U) **Overall Report Classification.** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category**. Joint Warfighting and Readiness

(U~~//FOUO~~) **Follow-Up Inspection of NSA/CSS Accuracy in Aligning Military Joint Duty Assignments with Billet Specifications**; NSA/CSS; IN-08-0003; 24 January 2008

(U~~//FOUO~~) **Summary.** The inspection, conducted in August 2007, was a follow-up review of an earlier OIG recommendation concerning NSA's compliance with a limited aspect of military joint duty assignment (JDA) regulations. The main areas for improvement cited in the inspection include: 1) establishing uniform expectations of Officer Assignment Managers' roles and responsibilities by setting verification frequency dates and assigning explicit JDA billet authorities; 2) adhering to the NSA Personnel Management Manual, Chapter 201, when reassigning JDA officers; and 3) finalizing the Certification Plan, which has been in draft since 2006.

(U) **Management Action.** Management concurred with the recommendations and is taking corrective action.

(U) **Overall Report Classification.** CONFIDENTIAL

(U) **Category**. Human Capital

(b) (3)-P.L. 86-36

(U) **Advisory Report on TURBULENCE Program Management**; NSA/CSS IG; AU-08-0007; 11 February 2008

(U~~//FOUO~~) **Summary.** A centerpiece for Agency transformation is the development of a series of mission modernization capabilities known as TURBULENCE. TURBULENCE focuses on the development and fielding of an architectural framework to modernize mission capabilities in a distributed, peer-to-peer, real-time environment. When TURBULENCE moved from research to development, it became part of the [redacted] On 9 January 2008, the first increment of [redacted] known as Increment I Passive, was granted approval by the Milestone Decision Authority to proceed to the next phase, system development and demonstration. Our advisory audit reported that the Agency must commit to full and timely TURBULENCE implementation through the [redacted] program. Although concrete steps have been taken to increase program

management rigor, only the initial [redacted] increment has been defined, and funding for a critically-related IT infrastructure project is in question. Program management is also [redacted] to support program operations. As a result of these findings, the OIG will begin a series of reviews for this fiscal year on selected areas of [redacted]

(U) **Overall Report Classification**. TOP SECRET//COMINT//NOFORN

(U) **Category**. Joint Warfighting and Readiness

(U) **Signals Survey and Analysis Division Within the Office of Target Pursuit**; NSA/CSS IG; IN-07-0004; 6 March 2008 (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Summary.** The inspection reviewed the Signals Survey and Analysis (SSA) Division for efficiency, effectiveness, and compliance, and to determine the relationship between SSA and the [redacted] and the functional boundaries between SSA and [redacted] Our inspection found a lack of strategic direction for the SSA workforce. Existing strategic plans do not address the role of signals analysis or SSA specifically. Since the inspection, SSA leadership has drafted a strategic plan that details specific objectives and measurements for the SSA workforce. Although SSA and [redacted] share compatible missions, their organizational separation hampers dialogue and limits operational collaboration. Finally, we found that SSA's relationship with [redacted] is inconsistent and collaboration is limited. While the relationship has improved with the division's renewed focus on the Centers, interaction is still based primarily on personal networks.

(U) **Management Action.** Agency management concurred with the recommendations.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, FVEY

(U) **Category**. Joint Warfighting and Readiness

(U) **Oversight Review of Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop**; NSA/CSS IG; AU-08-0015; 7 March 2008

(U//~~FOUO~~) **Summary.** The financial statements of the Agency's Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop were audited by a Certified Public Accountant firm (CPA) who issued unqualified opinions. Our oversight review of the CPA audit found that the audit was conducted consistent with Government Auditing Standards. Last year, the CPA audit made four recommendations: (1) require contract auditors to be on-site to observe year-end inventory closeout, (2) require Sodexho to fulfill its contractual obligation to provide an annual audited profit and loss statement to the Restaurant Fund, (3) maintain and track fixed asset records in one database, and (4) require Nonappropriated Fund Instrumentality (NAFI) managers to supervise inventory counts and verify that inventory counting procedures are followed. NAFI management has addressed and corrected each of these recommendations. The CPAs did not identify any management concerns this year.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category**. Financial Management

(U) **Agency's Transition to Internet Protocol Version 6**; NSA/CSS IG; AU-08-0004; 26 March 2008

(U//~~FOUO~~) **Summary.** The audit objective was to determine the Agency's progress in transitioning to Internet Protocol Version 6 (IPv6) and fulfilling the Information Assurance (IA) requirements established by the DoD and Director of National Intelligence. The Information Assurance Directorate has proven to be a valuable IA resource for the overall transition effort. However, NSA's transition status stands in contrast to the Office of Management and Budget's FY2007 assessment that more than half of the agencies are on track to meet the deadline. Our audit concluded that the Agency's transition to IPv6 has been stalled. The transition plan has not been approved by the Chief Technology Officer, and the Agency lacks a Program Management Office to manage and coordinate the transition to IPv6. We also found that recently acquired Information Technology (IT) devices may not process both IPv6 and its predecessor. By accepting the risk that IT devices may not process both, the Agency could delay implementation and incur increased costs.

(U) **Management Action.** The Technology Directorate (TD) concurred with our recommendations, and the IAD agreed to assist TD with information assurance support on IPv6 transition efforts.

(b) (3)-P.L. 86-36

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category**. Joint Warfighting and Readiness

(U) **Vehicle and Driver Services**; NSA/CSS IG; AU-08-0003; 31 March 2008

(U//~~FOUO~~) **Summary.** The audit objective was to determine whether the Agency operates an efficient and effective vehicle program. As of September 2007, the Agency owned [redacted] vehicles and transportation assets. In addition, the Agency leased [redacted] vehicles and assets. Our audit found that, with few exceptions, Commuter and Motorfleet Services does not operate an efficient vehicle program of almost [redacted] vehicles and assets. In FY2007 the Agency spent over [redacted] on vehicles and maintenance. However, more than half of the Agency vehicles reviewed had been used less than 50 percent of DoD's mileage guidelines. The Agency does not have a process for reviewing usage to determine whether or not a vehicle is needed or whether vehicles should be leased or purchased. Consequently, the Agency is leasing transportation assets that would be more cost-effective if purchased.

(U) **Management Action.** Management concurred with all recommendations and corrective actions are underway.

(U) **Overall Report Classification.** SECRET//REL TO USA, FVEY

(U) **Category**. Other (Logistics Services)

(U) **Procurement Fraud Initiative**; NSA/CSS IG; Various Control Numbers; 1 October 2007 to 31 March 2008

(U//~~FOUO~~) **Summary.** In October 2007, we launched an initiative to identify fraudulent billings by NSA contractors. This initiative involves data interrogation of contractor

access records, coordination with contractor compliance officials, analysis of billing records, and investigation of access and billing anomalies.

(U//~~FOUO~~) After a six-month run, our initiative has produced significant results. To date, we have identified several hundred potential mischarging matters, opened 38 new mischarging investigations, and completed 14 mischarging investigations, in which we substantiated more than 4,400 mischarged hours, amounting to approximately $500,000 in potential recoveries.

(U//~~FOUO~~) We are closely coordinating this initiative with the Defense Criminal Investigative Service, Baltimore, and the Office of the United States Attorney for the District of Maryland.

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U) **Advisory Report on NSA Participation in the Terrorism Watchlisting Process;** NSA/CSS IG; ODNI IG; JT-07-0006; 4 December 2007

(U//~~FOUO~~) **Summary.** In December 2006, the Intelligence Community Inspectors General Forum agreed to coordinate a review of the processes for nominating individuals to the consolidated terrorist watchlist. This advisory report responds to the Forum's Memorandum of Understanding, 19 March 2007 (amended and restated as of 7 May 2007), that required the NSA Office of the Inspector General to participate in a joint review. A team of inspectors from the ODNI and NSA conducted a joint review of NSA's participation in the terrorist watchlist nomination process from March to September 2007. The advisory report highlighted that: 1) no formal process exists for the review of [redacted] 2) no standardized format exists for submitting watchlist nominations; and 3) no Intelligence Community-wide training is available on the watchlist nomination process. These observations were included in the ODNI's inspection report, *Intelligence Community-Wide Review of the Terrorist Watchlist Nomination Process: Findings and Recommendations for Action*, 28 February 2008.

(U) **Management Action.** Management has initiated action in several areas highlighted by the joint IG team.

(U) **Overall Report Classification.** SECRET//NOFORN (b)(3)-P.L. 86-36

(U) **Category.** Joint Warfighting and Readiness

(U) **Geospatial Exploitation Office;** NSA/CSS IG; IN-06-0005; 22 January 2008

(U//~~FOUO~~) **Summary.** During an OIG organizational inspection, the Geospatial Exploitation Office [redacted] Nevertheless, the recommendations in the final report still apply to the GEO mission. Our inspection found that Signals Intelligence Directorate (SID) leadership concurs with the need to define and disseminate a clear division of effort across the Extended Enterprise. Since the on-site phase of the inspection, SID's Office of Analysis and Production's [redacted] of the GEO mission addressed many problems. However, throughout the inspection, SID was unable or unwilling to exercise any authority over the geospatial exploitation mission conducted in [redacted] GEO training, particularly for [redacted] must be relevant and formalized.

(U) **Management Action.** SID Management concurred with the recommendations. Although SID did not provide final action plans on several recommendations made in the draft report, the IG published the final report, including estimated completion dates, and will address those recommendations during the follow-up phase.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Joint Warfighting and Readiness

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

(b)(3)-P.L. 86-36

(U) ***For the Period April 1, 2007 Through September 30, 2007***

(U) **Government Purchase Card Program;** NSA/CSS IG; AU-06-0016; 12 April 2007

(U//~~FOUO~~) **Summary.** Our audit found that the Agency has successfully implemented a Government Purchase Card program and, for the most part, has effective controls over the [redacted] in annual purchases for FY2006. Unlike many agencies, NSA only issues credit cards to a small percentage of personnel; this limits financial exposure to wrongdoing and inadvertent misuse. Cardholders and certifying officials praised the program coordinators for their helpfulness and responsiveness. Nevertheless, the control environment needs strengthening in certain areas, including enforcement of requirements to get information technology purchases approved.

(U) **Management Action.** Management concurred with all recommendations to strengthen the control environment.

(U) **Overall Report Classifications.** SECRET//NOFORN

(U) **Category.** Acquisition Processes and Contract Management

(U) **Oversight Review of Restaurant Fund, Civilian Welfare Fund, and Gift Shop;** NSA/CSS IG; AU-07-0014; 15 May 2007

(U) **Summary.** The financial statements of the Agency's Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop were audited by a Certified Public Accountant (CPA) firm who issued unqualified opinions. Our oversight review of the CPA audit found no problems in the conduct of the audit by the CPA firm. The two problems reported last year - the need for a new Nonappropriated Fund Instrumentality (NAFI) contract and the need for a high-speed Internet connection - have been addressed. Additional concerns identified in the current year's report are: 1) the restaurant contractor did not submit an annual audited profit and loss statement as required; 2) contracted CPAs were not on-site to observe the year-end closeout inventory; 3) records are not maintained and tracked in one dedicated database; and 4) NAFI management did not observe inventory counts to ensure adherence to prescribed procedures.

(U) **Management Action.** Management is in the process of implementing the audit recommendations.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Financial Management

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~20291123~~

(U) **Chemical, Biological, Radiological, Nuclear Terrorism**; NSA/CSS IG; IN-06-0002; 24 May 2007

(b) (1)
(b) (3)-P.L. 86-36

(~~C//REL~~) **Summary.** As "the nexus between terrorism and weapons of mass destruction," the Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism mission is vital to national security. Our functional inspection of CBRN found that the CBRN workforce at NSA/CSS Washington (NSAW) and the Cryptologic Centers (CCs) is very talented and dedicated.

(U) **Management Action.** Management concurred in the recommendations and is taking corrective action.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Joint Warfighting and Readiness

(U) **SIGINT Dissemination for Analytic Collaboration per USSID CR1611(P);** NSA/CSS IG; ST-06-0017; 25 May 2007

(U) **Summary.** Provisional United States Signals Intelligence Directive (USSID) CR1611, *SIGINT Dissemination for Analytic Collaboration*, implements policy for the dissemination of SIGINT, either as a product or service, or for analytic collaboration. The USSID has been provisional since 2004. Our special study found that it does not institute adequate internal controls and implementation procedures are unclear and inconsistent with NSA dissemination practices. As a result, NSA cannot account accurately for SIGINT disseminated under the USSID and there are inconsistent interpretations of what constitutes appropriate dissemination during collaboration activities. If SIGINT is disseminated before it is minimized for U.S. Person information, violations of Legal Compliance and Minimization Procedures (USSID SP0018) could occur.

(U) **Management Action.** The Signals Intelligence Directorate (SID) management concurred with the report's finding and recommendations. SID agreed to reissue the USSID, establish a plan to educate the workforce on USSID standards, and establish quality control of SIGINT disseminations during analytic collaboration. These actions will reduce, but not eliminate, the risk.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Joint Warfighting and Readiness

(U//~~FOUO~~) **Mission Operations at the** ; NSA/CSS IG;

(~~C//REL TO USA, AUS, CAN, GBR, NZL~~) **Summary.** The NSA/CSS OIG conducted this assessment of Mission Operations and Governance at the concurrent with the U.S. Army Intelligence and Security

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123~~

Command (INSCOM) inspection of the [redacted] Overall, the [redacted] is performing at an exceptional level given its limited resources. However, the success of the [redacted] transition and the site's ability to take on additional mission responsibility hinges on clearly defined authorities, responsibilities, and sufficient resources. Our inspection also found that the lack of a clearly defined and documented management structure within [redacted] is causing confusion for the workforce and thereby negatively impacting current operations; reporting deficiencies were noted due to gaps in reporting expertise at the site; and critical programming and manpower actions must be completed in the near term for [redacted] to attain and sustain the [redacted] Center mission requirements as set forth in the concept plan.

(~~C//REL TO USA, AUS, CAN, GBR, NZL~~) **Management Action.** SID Management concurred with all findings. [redacted] management non-concurred with one of the findings; however, the site is already attempting to clarify the leadership roles to the workforce, as recommended.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(U) **Advisory Report on the Research Project on Governance for Agency Programs**; NSA/CSS IG; AU-07-0003; 22 June 2007

(b) (1)
(b) (3)-P.L. 86-36

(~~S//REL TO USA, AUS, CAN GBR, NZL~~) **Summary.** At the request of NSA's Deputy Chief of Staff, the OIG performed this review to determine what acquisition oversight is being performed over the [redacted] in FY 2007 Research, Development, Test & Evaluation funds. We concluded that almost all of the funds received some degree of oversight by the Directorate of Acquisition (DA) and that the Agency improved this oversight by: 1) increasing the number of Program Executive Offices (PEOs) in the new DA organizational structure from [redacted] 2) creating the Tier 1 list of programs (major investment programs that are critical to NSA's transformation and are directly managed by the PEOs); and 3) implementing new acquisition guidance.

(U) **Overall Report Classification.** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category.** Acquisition Processes and Contract Management

(U//~~FOUO~~) **Satellite Modernization – [redacted] Program Management**; NSA/CSS IG; [redacted]

(~~S//REL TO USA, AUS, CAN, GBR, NZL~~) **Summary.** The Program Management Office (PMO) for Satellite Modernization – [redacted] has demonstrated effective leadership, strong communication with the partners, and innovative, cost-effective solutions to technical issues in managing this critical program, valued at approximately [redacted] However, our audit found that collaboration with the [redacted] partners is impeded by the conflicting standards and requirements of each participating partner, which the PMO is responsible for resolving. Additionally, based on two of the dollar thresholds specified in Department of Defense Instruction 5000.2, *Operation of the*

(b) (3)-P.L. 86-36

Defense Acquisition System, as implemented by NSA/CSS Policy 8-1, the SV program

[redacted]

(U//~~FOUO~~) **Management Action.** The actions taken by the Senior Acquisition Executive meet the intent of the recommendations on the acquisition issues. The Office of the Director of National Intelligence will not include the SV Program on the Major System Acquisition list because it is too far along in the acquisition cycle. NSA's Office of Policy & Records provided an alternate recommendation addressing partnership concerns. Therefore, the OIG is referring this recommendation to the Chief Technology Officer for action.

(U) **Overall Report Classification.** TOP SECRET//COMINT//REL TO USA, FVEY

(b) (1)
(b) (3)-P.L. 86-36

(U) **Category**. Acquisition Process and Contract Management

(U) **FY2007 Report on Compliance with the Federal Information Security Management Act at NSA/CSS**; NSA/CSS IG; AU-07-0009; 31 July 2007

(~~C//REL TO USA, AUS, CAN, GBR, NZL~~) **Summary.** Our FY2007 report on compliance with the Federal Information Security Management Act at NSA/CSS concluded that the Agency is making steady improvements to the security posture of its systems and networks. However, much more work must be done to [redacted]

[redacted]

(U) **Management Action.** Management concurred with the recommendations and continues to take corrective action.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Information Security and Privacy

(U) **Mission Alignment and Build Out**; NSA/CSS IG, ST-07-0005; 6 August 2007

(U//~~FOUO~~) **Summary.** The IG team began its special study of Mission Alignment and Build Out in April 2007. The special study was undertaken, in part, because information gathered from field and HQ inspections pointed to some human resource, mission delegation, and roles, responsibilities, and authorities issues of vital importance to Agency transformation. Shortly after the study was initiated, the Signals Intelligence Directorate (SID) reapportionment discussions were made public. As our review progressed, it became clear the SID reapportionment would significantly affect our results. Although we curtailed the study, we had gathered sufficient data to offer observations

(b) (3)-P.L. 86-36

highlighting some systemic governance and manpower issues. We found confusion about and inconsistencies between Enterprise governance policies and directorate-level implementing documents. Disciplined processes, an accurate mechanism to track and maintain data on human resources, and the commitment of leadership would enhance the Mission Alignment and Build Out initiative's ability to meet Transformation goals. While we did not make specific recommendations, we noted areas in need of leadership attention to help ensure a unified Global Enterprise.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Joint Warfighting and Readiness

(b) (1)
(b) (3)-P.L. 86-36

(~~C//REL TO USA, AUS, CAN GBR, NZL~~) [redacted]
NSA/CSS IG; AFISRA; NNWC; [redacted]

(~~C//REL TO USA, AUS, CAN GBR, NZL~~) **Summary.** The IG organizations of the NSA/CSS IG, Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA), and the Naval Network Warfare Command (NNWC) performed the first joint inspection of

[redacted]

(U) **Management Action.** Management concurred with the findings of the joint inspection team and is taking corrective action.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

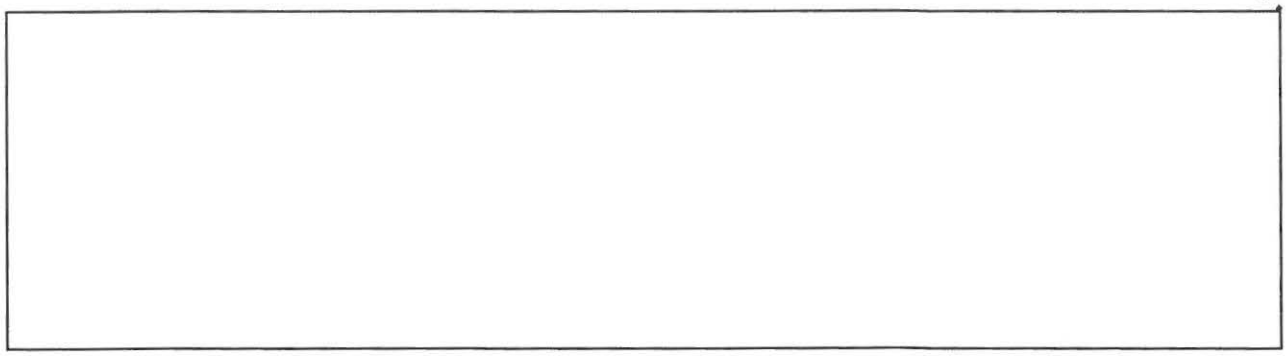
(U) **Category.** Joint Warfighting and Readiness

(U) **SIGINT Voice Processing System;** NSA/CSS IG; AU-07-0015; 22 August 2007

(~~S//REL TO USA, AUS, CAN, GBR, NZL~~) **Summary.** [redacted]

[redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36



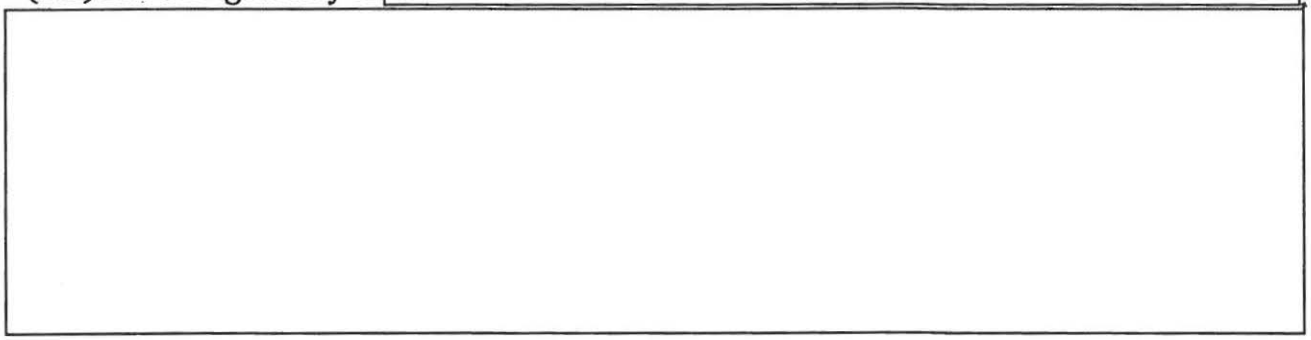
(U) **Management Action.** Management concurred with all recommendations and corrective actions are underway.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, FVEY

(U) **Category.** Joint Warfighting and Readiness

(U) **Acquisition Management;** NSA/CSS IG; AU-07-0002; 23 August 2007

(~~C//REL TO USA, AUS, CAN, GBR, NZL~~) **Summary.** The Directorate of Acquisition (DA) has a long history of



(U) **Management Action.** Management concurred with all recommendations and has initiated or planned actions in response to the audit findings.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Acquisition Processes and Contract Management

(U) **Advisory Report on the Followup Research of Activities Associated with Expeditionary SIGINT Deployments to Hostile Areas**; NSA/CSS IG; ST-07-0015; 24 August 2007

(U//~~FOUO~~) **Summary.** This followup research continues the Office of the Inspector General's examination of the processes associated with the deployment of NSA/CSS personnel to hostile areas in the Central Command Area of Responsibility (CENTCOM AOR). A 2006 IG report *(Advisory Report on the Activities Associated with Expeditionary SIGINT Deployments to Hostile Areas)* highlighted the need to standardize processes related to candidate selection, pre-deployment mission training, Information Technology (IT) support and corporate resolution of issues. For the followup, we evaluated data

provided by interviews and a web survey with NSA/CSS personnel who deployed to [redacted] In addition, we interviewed representatives of organizations involved in the deployment process. We found that, overall, major process improvements have been made, particularly administrative processes consolidated by the NSA Deployment and Readiness Center. However, several areas require continued monitoring: mission training; IT investment; P3 performance review, and oversight of time and attendance.

(U) **Management Action.** Management concurred in the recommendations and is taking corrective action.

(U) **Overall Report Classification.** SECRET//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(U) **Menwith Hill Station**; AFISRA IG; NNWC IG; INSCOM IG; NSA/CSS IG; Other IG; JT-07-0003; 13 September 2007

(~~S//REL TO USA, AUS, CAN GBR, NZL~~) **Summary.** The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA), Naval Network Warfare Command (NNWC), Intelligence and Security Command, NSA, and another IG visited Menwith Hill Station (MHS) in June 2007. The joint IG team found that MHS has demonstrated exceptional mission success and outstanding contributions to the SIGINT effort in [redacted] Higher HQ and MHS leaders have taken remarkable steps since our last joint inspection in 2004 to effectively integrate and synchronize operations and support in a demanding environment. The following recommendations merit management's attention: [redacted]

(U~~//FOUO~~) **Management Action.** Management concurred with the findings of the joint inspection team and is taking corrective action.

(U) **Overall Report Classification.** SECRET//COMINT//TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL (b)(1) (b)(3)-P.L. 86-36

(U) **Category.** Joint Warfighting and Readiness

(U) **Status of Agency Study on Information System Security**; NSA/CSS IG; AU-07-0001; 14 September 2007

~~(S)~~ **Summary.** The audit determined whether the Agency had taken steps to implement the [redacted] recommendations for strengthening the Agency's information system security posture. While our initial focus was to identify the status of the [redacted] Our review found that since 2000, numerous Agency studies, reports, and assessments of the

(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

vulnerability of Agency Information Systems have been conducted [redacted]

[redacted]

(U//~~FOUO~~) **Management Action.** The Information Technology and Information Assurance Directorates agreed to implement corrective action for all of the recommendations.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Information Security and Privacy

(U) **Labor Mischarging;** NSA/CSS IG; IV-07-0052; 12 September 2007

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that a contract employee mischarged an NSA Time and Materials contract between January 2006 and June 2007. We determined the contract employee mischarged 270 hours, amounting to approximately $22,000 in false billings. The contractor reimbursed NSA that amount and dismissed the employee. The United States Attorney's Office, District of Maryland, declined prosecution due to the contractor's cooperation and reimbursement to NSA.

(U) **Management Action.** The matter was referred to the ADS&CI for possible security clearance action. The company made restitution in accordance with our findings.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category**. Other (Contract Fraud)

(U) **Falsification of Crypto-Tape Testing Documents;** NSA/CSS IG; IV-07-0036, 30 August 2007

(b) (3)-P.L. 86-36

(U//~~FOUO~~) **Summary.** The NSA OIG conducted an investigation in response to an allegation that an Agency Cryptologic Fabrication worker forged the initials of two Agency officials responsible for conducting quality control tests on secure communications tapes ("crypto tapes"). According to the complainant, the subject employee forged the two officials' initials on quality control documents, but no quality control testing had been conducted. Our investigation substantiated the allegation. [redacted] The forged testing records were discovered prior to shipment, and we verified that this lot of tapes received appropriate quality control testing before it was released for distribution. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The Report of Investigation in this matter was referred to the NSA Associate Directorate for Security and Counterintelligence (ADS &CI) for possible action on the employee's security clearance, and to NSA Employee Relations for administrative discipline.

(U) **Overall Report Classification**. UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Falsification)

(U) **Falsification of Medical Center Document**; NSA/CSS IG; IV-07-0028; 15 June 2007

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that an NSA employee falsified an official Government document in order to misrepresent her whereabouts to Agency management. The employee admitted she intentionally altered an Agency official's writing on an Occupational Health, Environmental & Safety Services document. The NSA OIG previously substantiated significant time and attendance violations against this particular employee.

(U) **Management Action.** The NSA OIG Report of Investigation on this matter was referred to the ADS & CI for possible action on the employee's security clearance and to NSA Employee Relations for administrative discipline.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Falsification)

(U) **Travel Voucher Fraud and Misuse of Government Charge Card**; NSA/CSS IG; IV-07-0007; 30 August 2007

(U//~~FOUO~~) **Summary.** The NSA OIG conducted an investigation in response to an allegation that an NSA Computer Scientist altered TDY itineraries and charged the Government for post-TDY "Rest and Relaxation" (R&R) trips to Thailand. Our investigation substantiated that the employee altered his official itineraries on four separate occasions to add a total of eight post-TDY R&R trips to Thailand. We determined the Government paid the employee's airfare for seven of these eight R&R trips, and that the employee inappropriately charged airfare for all eight trips to his Government travel charge card. In addition to the cost of the airfare for the Thailand trips, a review of 38 travel vouchers submitted by the employee between 2004 and 2007 determined that the employee was mistakenly reimbursed for other non-reimbursable TDY expenses. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** Our Report of Investigation in this matter was referred to the ADS&CI for possible action on the employee's security clearance; to NSA Employee Relations for administrative discipline; and to the NSA Travel Card Program Office for initiation of a restitution action. The Agency has suspended the employee's Government travel charge card.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Travel Voucher Fraud / Misuse of Resources)

(U) **Time & Attendance Fraud, Travel Voucher Fraud, Misuse of Government Charge Card**; NSA/CSS IG; IV-06-0057; 31 August 2007

(U//~~FOUO~~) **Summary.** The NSA OIG conducted an investigation based upon

allegations of voucher fraud against a GG-13 [redacted] We substantiated that the employee: 1) intentionally falsified her timesheets, for a total shortfall to the Government of 360.50 hours (approximately $15, 580); 2) intentionally falsified a Government travel voucher, charging the Government $1,001.40 for expenses in Hawaii when the trip was essentially a personal vacation; and 3) intentionally misused her Government travel charge card. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The OIG Report of Investigation was referred to the ADS&CI, for possible security clearance action; to NSA Employee Relations for administrative discipline; and to the NSA Office of Finance for initiation of a restitution action.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Fraud and Misuse)

(U) **Government Credit Card Misuse**; NSA/CSS IG; IV-07-0035; 17 September 2007

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that a former military assignee at NSA (now a contractor assigned to an NSA contract) knowingly misused his Government-issued travel charge card by charging over $23,000 in personal expenses to the card, including a $21,700 charge for on-line foreign currency trading, $1,403.50 for cash advances and $54.00 for cinema tickets. The former assignee failed to pay a balance of $14,262.95 on the card prior to leaving Government service. The OIG verified that the former assignee is personally responsible for this debt, and therefore there is no potential pecuniary loss to the Government. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The NSA OIG's Report of Investigation in this matter was referred to the ADS&CI for possible security clearance action.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Misuse of Resources)

(U) **Misuse of Agency Software**; NSA/CSS IG; IV-07-0019; 23 July 2007

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that a GG-14 employee removed unused, unclassified Government-owned Commercial-Off-the-Shelf (COTS) software from Agency spaces, without authorization, and then installed the software on multiple personally owned computer systems. We also determined that, after installing the COTS software, the employee and/or a family member activated it, rendering it useless to the Agency. Finally, we concluded the employee failed to fully and truthfully respond to management inquiries about the COTS software.

(U) **Management Action.** The Report of Investigation in this matter was referred to the ADS&CI for possible security clearance action, and to NSA Employee Relations for administrative discipline. We also referred the matter to the Agency's Office of Finance for initiation of a restitution action.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Misuse of Resources)

(U) **Misuse of NSA Computer Networks**; NSA/CSS IG; IV-07-0024; 10 September 2007

(b) (6)

(U//~~FOUO~~) **Summary.** The NSA OIG substantiated an allegation that a GG-13 Skills Community Director misused Government resources for private gain. Our investigation determined that the employee used the classified and unclassified computer networks to facilitate [redacted]

(U) **Management Action.** The matter was referred to NSA Employee Relations for administrative discipline.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Misuse of Resources)

(U) **Misuse of NSA Unclassified Computer Network**; NSA/CSS IG; Various Control Numbers; 1 April 2007 to 30 September 2007

(U) **Summary.** During the past six months, the NSA OIG substantiated a total of 33 allegations that NSA affiliates misused Government resources by accessing adult-oriented material on the Agency's unclassified computer network. The 33 cases break down as follows: 18 contractor matters, 8 military assignee matters and 7 civilian matters.

(U) **Management Action.** Consequences for contractor employees ranged from company reprimand to dismissal from employment. Military assignee cases were referred to the appropriate service for military discipline. Civilian cases were referred to NSA Employee Relations for administrative discipline. All matters were referred to ADS&CI for possible security clearance action.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Misuse of Resources)

(U) **Child Pornography**; NSA/CSS IG; CO-07-0279; 5 March 2007

(U//~~FOUO~~) **Summary.** The NSA OIG supported an FBI investigation into an NSA/CSS GG-15 civilian employee [redacted] The FBI's investigation was part of Project Safe Childhood, a nationwide initiative designed to protect children from online exploitation and abuse. An FBI search of the civilian's Maryland residence and analysis of his home computer revealed that he used his home computer to receive more than [redacted] images of child pornography from the Internet. On [redacted] he was sentenced in Federal court to [redacted] years in prison followed by [redacted] years of supervised release for receipt of child pornography. He was also ordered to register as a sex offender.

(U) **Management Action.** The employee is no longer employed at the Agency and does not hold a security clearance.

(b) (6)

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Child Pornography)

(U) **Misrepresentation of Academic Credentials;** NSA/CSS IG; IV-07-0003 (8 August 2007); IV-07-0009 (30 April 2007); IV-07-0025 (8 August 2007)

(U) **Summary.** A Federal law enforcement Agency provided the NSA OIG with a list of individuals who obtained bogus degrees from diploma mills. Through a data interrogation process, we were able to determine that the list contained the names of three NSA civilian employees. We determined that each employee paid a fee for a bogus degree and represented that degree to the Agency as legitimate. We also determined that the employees provided the Agency with academic transcripts setting forth courses they did not actually take and grades they did not actually receive. In each case, we concluded the employees either knew or reasonably should have known their degrees were illegitimate, and that they intentionally misrepresented their credentials and qualifications to the NSA.

(U) **Management Action.** The OIG's Reports of Investigation were referred to the ADS&CI for possible security clearance action; to NSA Employee Relations for administrative discipline; and to NSA Human Resources for any necessary grade and pay adjustments.

(U) **Overall Report Classification**. UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Misrepresentation)

(U) **Hostile Work Environment**; NSA/CSS IG; IV-07-0027; 6 June 2007

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a GG-15 manager at an Agency field site created a hostile work environment for one of the military assignees. Our investigation determined that the GG-15's performance frustrations with the military assignee caused him to make statements and gestures toward the military member that were abusive in nature. We concluded that the GG-15 violated applicable NSA Policy by using intimidating language and gestures, and failing to exercise courtesy and respect in dealing with a coworker.

(U) **Management Action.** The OIG Report of Investigation in this matter was referred to NSA Employee Relations for administrative discipline.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Hostile Work Environment)

(U) **Time and Attendance Fraud**; NSA/CSS IG; IV-07-0011; 05 May 2007

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that, between 1 February 2006 and 19 January 2007, a GG-13 Facilities Project Manager intentionally submitted false and inaccurate timesheets, for a total shortfall to the Government of 646 hours (approximately $28,824). The employee asserted that he regularly conducted NSA business from inside his car in the NSA parking lot (outside the NSA CONFIRM

(b) (6)

system), because [redacted] Our investigation determined this explanation was implausible. The United States Attorney's Office, District of Maryland, declined prosecution in favor of administrative discipline.

(U) **Management Action.** The OIG Report of Investigation was referred to the ADS&CI for possible security clearance action; to NSA Employee Relations for administrative discipline; and to the NSA Office of Finance for initiation of a restitution action.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Time and Attendance)

(b) (3)-P.L. 86-36

(U//~~FOUO~~) **Financial Accountability** [redacted] NSA/CSS IG;

[redacted]

(~~C//REL TO USA, AUS, CAN, GBR, NZL~~) **Summary** [redacted]

(U) **Management Action.** Responsible contractor made restitution in accordance with OIG findings.

(U) **Overall Report Classification.** TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Other (Financial Accountability)

(b) (1)
(b) (3)-P.L. 86-3

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) **Inspection of the Geospatial Exploitation Office**; NSA/CSS IG; IN-06-0005

(~~C//REL TO USA, FVEY~~) **Background.** The Geospatial Exploitation Office (GEO) began operations [redacted] The primary objectives of the inspection were to assess GEO's mission effectiveness, GEO's ability to satisfy requirements and information needs levied on the organization, and GEO mission management. Prior to publication of the draft report, the SIGINT Directorate's Deputy Director for Analysis and Production realigned the S2 organization. The realignment resulted in [redacted] Several findings and recommendations were identified in the draft inspection report that apply to the GEO mission as a whole and not the GEO organization in particular. Depending on the outcome of the draft report review process, these mission topics may need to be addressed at the SID level.

(b)(3)-P.L. 86-36

(U) **Special Studies of Counterterrorism Programs**; NSA/CSS IG

(U//~~FOUO~~) **Background.** In January 2007, all Counterterrorism programs previously operated under Presidential authority began operating under the authority of Foreign Intelligence Surveillance Court orders. For these new orders, the OIG performed reviews in accordance with their terms, which specified that an initial review would be done to ensure that minimization procedures were adequate. The FISC orders imposed strict time limits, but when possible, these reviews included testing. The OIG completed two such reviews in the past six months. In addition, we published a report on a special inquiry performed to answer concerns raised about activities under one of the FISC orders.

(U) **Assistance to ODNI IG for the Terrorist Watchlist Project;** NSA/CSS IG; JT-07-0006

(U) **Background.** The Terrorist Screening Center (TSC) maintains a consolidated terrorism watchlist that is populated by information from the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI). Agencies that possess or acquire terrorism and counterterrorism information, with the exception of purely domestic counterterrorism information, are required by Executive Order 13354 to promptly give access to such information to the NCTC. The NCTC provides a subset of that information to the TSC for inclusion on the consolidated watchlist. The Intelligence Community Inspectors General (ICIG) Forum agreed to coordinate a review of the processes for nominating individuals to the consolidated terrorist watchlist. The Offices of the Inspector General of the Office of the Director for National Intelligence (ODNI), Central Intelligence Agency (CIA), Department of Justice (DOJ), Defense Intelligence Agency (DIA), National

Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), Department of State (State), Department of Homeland Security (DHS), Department of Energy, and Department of Treasury (Treasury) are participating in the joint review. While other IC agencies performed internal reviews within their respective agencies, ODNI and NSA inspectors jointly reviewed NSA's participation in the watchlisting nomination process. The joint inspection team focused on the provision of terrorist-related SIGINT information to the NCTC for the purpose of watchlisting. Cross-community findings and observations from the individual agency reports will be incorporated in the overall IC IG report.

~~SECRET//REL TO USA, FVEY~~

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) ***For the Period April 1, 2008 through September 30, 2008***

(U) Assessment of Management Controls to Implement the Protect America Act of 2007; **NSA/CSS IG; ST-08-0001; 3 April 2008**

(U//~~FOUO~~) Summary. NSA has implemented procedures to comply with the provisions with the Protect America Act of 2007 (PAA), which modified the Foreign Intelligence Surveillance Act (FISA) and was signed into law on 5 August 2007. To protect the privacy rights of U.S. persons, the new legislation required NSA to implement and follow procedures established by the Director, NSA, to ensure its adherence to three requirements: that targets are located overseas, that the foreign intelligence purpose is significant, and that personnel follow applicable minimization procedures. Our findings included: 1) NSA immediately implemented DIRNSA-directed procedures on compliance with PAA and strong controls to determine that targets are located outside of the U.S; 2) PAA tasking needs additional controls, in particular to verify that only authorized selectors are on collection and that the information acquired relates to the foreign intelligence target; and 3) more rigorous controls will increase the reliability of spot checks for PAA compliance.

(U) Management Action. **Management concurred with the recommendations.**

(U) Overall Report Classification. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Significantly Improve Intelligence Capabilities**

(U) NSA/CSS Hawaii; **NSA/CSS IG; AFISRA IG; INSCOM IG, NNWC IG; INSCOM; JT-08-0001; 23 April 2008**

(U//~~FOUO~~) Summary. **The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency; Naval Network Warfare Command; Intelligence and Security Command; and NSA conducted the inspection at Kunia, Hawaii, in January and February 2008. The transformation challenges identified during the inspection of mission operations at NSA/CSS Hawaii (NSAH) are a microcosm of those facing the Extended Enterprise: the requirement to maintain legacy capabilities on critical enduring target sets and, at the same time, develop a workforce that can take on the challenges of the networked world. We found that** [redacted] **With the completion of the new NSAH building years away, the likelihood that personnel will have to remain in the tunnel past FY13 has emerged. An engineering and safety study of the tunnel has revealed several health and safety problems that must be addressed in the near term. Funding for these repairs must be identified as well. Finally, the inspection team identified fourteen commendable achievements across all elements of NSAH, reflecting solid leadership at all levels.**

(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: ~~20320108~~

(U) Management Action. **Management concurred with the recommendations and is taking corrective action.**

(U) Overall Report Classification. **TOP SECRET//COMINT//REL TO USA, FVEY**

(U) Category. **Joint Warfighting and Readiness**

(U) Official Representation and Confidential Military Funds; **NSA/CSS IG; AU-08-0017; 23 April 2008**

(U//~~FOUO~~) Summary. **We conducted this audit to determine whether Official Representation and Confidential Military Funds are managed consistent with laws and regulations and to follow-up on our previous audit recommendations. We found that NSA organizations, such as the Internal Review Group and Operations Risk Management, have conducted adequate internal-control reviews of the Official Representation and Confidential Military Funds. Therefore, we discontinued our audit. We will periodically review the Internal Review Group's accounting practices to ensure that adequate oversight continues.**

(U) Overall Report Classification. **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U) Category. **Financial Management**

(U) Advisory Report on NSA/CSS Extended Hours Operations; **NSA/CSS IG; ST-08-0003; 30 May 2008**

(U//~~FOUO~~) Summary. **Extended-hours areas include watch/operation centers, production areas, and support offices. We reviewed the consolidation achieved and efforts currently underway by the National Security Operations Center, Signals Intelligence Directorate, Technology Directorate, Information Assurance Directorate, and other Agency organizations. Our special study found that over the past 12-18 months significant progress in reducing and consolidating extended- hours organizations has been achieved. An interview of the Director of Installations and Logistics and the Special Executive for Power, Space, and Cooling revealed that recent consolidation efforts have produced available space for other uses and that extended-hours operations areas have minimal effect on power consumption. We also found that there is no single authority for establishing extended-hours operations, nor is there official policy or guidance for setting up or maintaining extended-hours areas or functions. Finally, NSAW does not maintain a consolidated list of extended-hours operations areas.**

(U) Overall Report Classification. **TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL**

(U) Category. **Joint Warfighting and Readiness**

(U) NSA/CSS Colorado; **NSA/CSS IG; AFISRA IG; INSCOM IG; JT-08-0002; 18 June 2008**

(U//~~FOUO~~) Summary. **The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency; Intelligence and Security Command; and NSA conducted the inspection at NSA/CSS Colorado (NSAC). This was the first inspection of NSAC. The**

inspectors found that confusion surrounding the NSAC mission, functional realignment, and implementation timing has created dissention and distrust that has diverted mid- and upper-level management's focus from the mission. We found a number of compliance problems typical of a site undergoing its first inspection. For example,

Finally, the inspection team identified three commendable achievements across all elements of NSAC.

(U) Management Action. Management concurred with the recommendations and is taking corrective action.

(U) Overall Report Classifications. **SECRET//COMINT//TALENT KEYHOLE//REL TO USA, FVEY**

(U) Category. **Joint Warfighting and Readiness**

(b) (3)-P.L. 86-36

(U) Closeout; NSA/CSS IG;

(U//~~FOUO~~) Summary. In May 2002, the Director, NSA notified the Assistant Secretary of Defense, Command Control, Communications and Intelligence, that the Our audit found that; overall, the Microelectronics Solutions organization has made little progress in the closeout of in accordance with applicable DoD and NSA/CSS regulations, especially in regard to the has done little to prepare the building for reutilization or to reduce its power consumption. This failure to act persists even though the operations ended and Microelectronics Solutions management has had to prepare for the shutdown. , the Agency has spent more than on this effort and,

(U//~~FOUO~~) Management Action. Management concurred with our recommendations, but advised us that power consumption was not a priority for the closure. Because of the Microelectronics Solutions management's inability to make any progress in the shutdown of we made a recommendation to the Information Assurance Director to restructure Microelectronics Solutions management that is responsible for the delay.

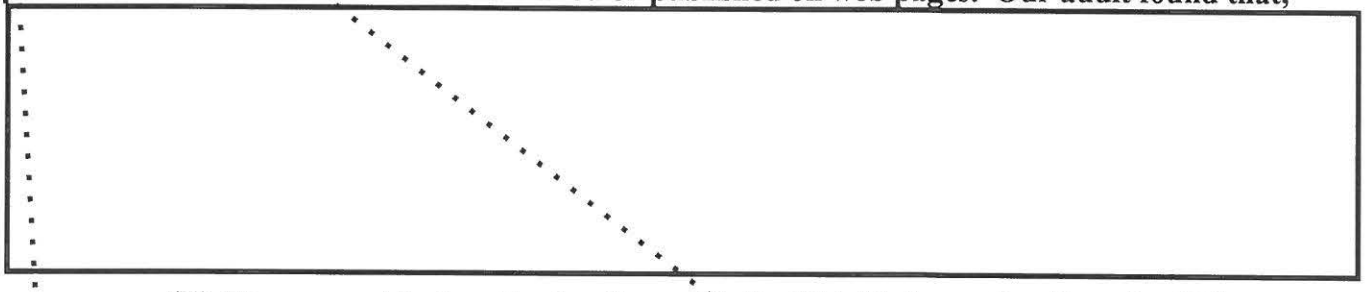
(U) Overall Report Classification. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(U) NSA's Top Secret /Special Compartmented Information Public Key Management Infrastructure; **NSA/CSS IG; AU-08-0001; 27 June 2008**

(b) (3)-P.L. 86-36

(U//~~FOUO~~) Summary. **NSA Public Key Infrastructure (PKI) protects NSA communications and networks by providing authentication of users, encryption, and digital signing. NSA PKI ensures that security restrictions on classified data and information are maintained when information is e-mailed or published on web pages. Our audit found that,**



(U) Management Action. **During the audit, the Chief Information Security Officer initiated actions to address the noted conditions.**

(U) Overall Report Classification. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(U) Nuclear Weapons Personnel Reliability Program; **NSA/CSS IG; AU-08-0006; 7 July 2008**

(U//~~FOUO~~) Summary. **One of the Agency's most important missions is** [redacted] **The purpose of the Nuclear Weapons Personnel Reliability Program (NWPRP) is to ensure that everyone who performs these duties meets the highest standards of reliability, including physical, psychological, and technical competence. The NSA/CSS Office of Inspector General, which is responsible for DoD oversight, has conducted periodic audits of the NWPRP since 2001. Our most recent audit found that the NWPRP has significantly improved the security, medical, and program management controls since our initial review in 2001. The program has established a systemic process to ensure and document that individuals accepted into the program meet, and continue to meet, DoD reliability standards. NSA policy requires that NWPRP employees be randomly drug tested at a higher rate than the rest of the Agency population. However, flaws in the selection methodology prevent the program from meeting its stated goals.**

(U) Management Action. **Management concurred with all recommendations and corrective actions are underway.**

(U) Overall Report Classification. **CONFIDENTIAL//REL TO USA, FVEY**

(U) Category. **Joint Warfighting and Readiness**

(U) RT-10 Initiative; **NSA/CSS IG; AU-07-0016; 11 July 2008**

(b)(3)-P.L. 86-36

~~(S//REL)~~ Summary. **To improve SIGINT support for the Joint Intelligence Operations Capability in Iraq, NSA developed a system called RT-10;** [redacted] **We performed this audit in response to an allegation that RT-10 had been developed without the programmatic oversight that NSA and DoD regulations require. We found this allegation** [redacted] **essential for an ongoing war. The Agency has recently made progress in establishing program structure for RT-10, an effort that should be reinforced as the system is** [redacted] **Our audit concluded that, since** [redacted] **the RT-10 program has operated without the oversight and documentation necessary to hold the Program Office accountable for cost, schedule, and performance. With DoD support, the program was expanded** [redacted] **although a Capability Production Document, the formal requirements specification, was not sent to DoD for validation until** [redacted]

(U) Management Action. **Management concurred with the recommendations.**

(U) Overall Report Classification. **TOP SECRET//COMINT-ECI RDV//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(U) [redacted] on the Agency's Unclassified Network; **NSA/CSS IG; AU-08-0005B; 14 July 2008**

~~(S//REL)~~ Summary. **In its current state, the Technology Directorate (TD)-developed** [redacted]

(U) Management Action. **The TD concurred with our recommendations, and the Signals Intelligence Directorate and NSA/CSS Threat Operations Center agreed to assist TD in the process. TD has started to take corrective actions.**

(b)(1)
(b)(3)-P.L. 86-36

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(U) Compliance with the Federal Information Security Management Act at NSA/CSS; **NSA/CSS IG; AU-08-0012; 31 July 2008**

(U//~~FOUO~~) Summary. **Our FY 2008 audit on compliance with the Federal Information Security Management Act found that, after another FISMA reporting cycle, the Agency has**

made some improvements to the security of its systems and networks. Information Technology (IT) security personnel are becoming more effective in [redacted] into major Agency initiatives. For example, [redacted] However, much more work must be done to correct the material weakness reported in August 2006 regarding IT security for systems within NSA's control. Weaknesses that have not been fully mitigated include: [redacted]

(U) Management Action. Management concurred with the recommendations and corrective actions are underway.

(U) Overall Report Classifications. TOP SECRET//COMINT//NOFORN

(b) (3)-P.L. 86-36

(U) Category. Information Security and Privacy

(U//~~FOUO~~) Advisory Report on the [redacted] NSA/CSS IG;

~~(S//REL)~~ Summary. To achieve its stated goal of [redacted] NSA has implemented a series of initiatives called Transformation 3.0. One initiative, [redacted] This advisory review focused on the Intelligence Oversight (IO) and internal controls implemented by [redacted] developers. Our review concluded that [redacted] developers are properly applying Signals Intelligence (SIGINT) rules to SIGINT activities and Information Assurance (IA) rules to IA-relevant activities and are implementing appropriate IO controls. However, not all IO controls have been documented or implemented because [redacted] is not yet fully operational under [redacted] Because [redacted] supports a new mission for NSA, and the risk is high if safeguards are not incorporated into procedures to ensure protection of U.S. persons information, an IO review of control mechanisms may be warranted when [redacted] becomes fully operational.

(U) Overall Report Classifications. TOP SECRET//COMINT//REL TO USA, FVEY

(U) Category. Significantly Improve Intelligence Capabilities

(U) [redacted] Project; NSA/CSS IG; [redacted]

~~(S//REL)~~ Summary. Our audit found that [redacted] which provides [redacted] Transformation 3.0 programs, is not adequately funded. Without adequate funding, critical components of the [redacted] program will fail. [redacted] is included in a set of projects called [redacted] Since the project began, [redacted] development costs have been [redacted] The [redacted]

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(U) Management Action. **Management agreed with our recommendations to improve the requirements and budget processes for the projects.**

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Significantly Improve Intelligence Capabilities**

(U) Agency's System Security Plans; **NSA/CSS IG; AU-08-0005A; 8 September 2008**

~~(S//REL)~~ Summary. **Since 2002, the Agency OIG has reported that deficiencies in the Agency's System Security Plans (SSP) Program Contributing factors include a lack of Agency requirements, standards, and resources. Our audit found that, although currently implementing initiatives to improve the SSP Program, We also determined that the Information Security Office did not establish a baseline level of evidence for all accreditation decisions.**

(U) Management Action. **The Technology Directorate concurred with our recommendations and has started to take corrective actions.**

(b) (3)-P.L. 86-36

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Information Security and Privacy**

(U) Utilization of Time and Material (T&M) Contracts; **NSA/CSS IG; AU-07-0006; 16 September 2008**

(U//~~FOUO~~) Summary. **We performed this audit as part of the Agency OIG's contract fraud initiative to determine whether controls are adequate for contractor oversight. Since 2005, NSA has collected or is in the process of collecting more than $1 million in contractor mischarging on service contracts, including T&M. Today the Agency has more than T&M contracts valued at about Our audit found that the Agency does not routinely perform the extensive oversight needed for T&M contracts, in spite of recent substantiated mischarging. Our review of contract actions confirmed this appraisal, especially in regard to certifying contractor invoices and validating contractor education and experience. The underlying cause of the contracting problems has been long-term understaffing of the Contracting Group. A recently approved FY2008 staffing increase to Acquisition should improve the Group's ability to work with Agency organizations to avoid T&M contracts and provide necessary oversight.**

(U//~~FOUO~~) Management Action. **The Director, Business Management Integration (BMI), has not provided comments to Recommendation 2 that Acquisition develop a plan to convert long-term T&M contracts to fixed-price contracts (including performance-based). We have again asked the BMI Director to respond to this report. The Contracting Group has taken or started to take corrective actions in response to our other recommendations. The Technology Directorate (TD) concurred with our recommendations, and the Signals Intelligence Directorate and NSA/CSS Threat Operations Center agreed to assist TD in the process. TD has started to take corrective actions.**

(U) Overall Report Classifications. **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U) Category. **Acquisition Processes and Contract Management**

(U) Joint Duty Assignment Program - Civilian; **NSA/CSS IG; ST-08-0020; 29 September 2008**

(U//~~FOUO~~) Summary. **Our special study on NSA's implementation of the Joint Duty Assignment (JDA) Program found that NSA is implementing the JDA program as effectively as possible given the evolving state of the JDA program within the Intelligence Community. DoD implementing guidance was issued on 2 June 2008; NSA's implementing guidance is currently in draft and is expected to be published shortly. However, we did identify the following concerns that may impede the JDA program: 1) The requirement to keep an individual on the losing organization's billet for the duration of the JDA tour, which may result in denial of the assignment, is a contentious issue; 2) JDA vacancies are not attracting candidates; and 3) JDA credit and waiver decisions are delayed awaiting policy and guidance.**

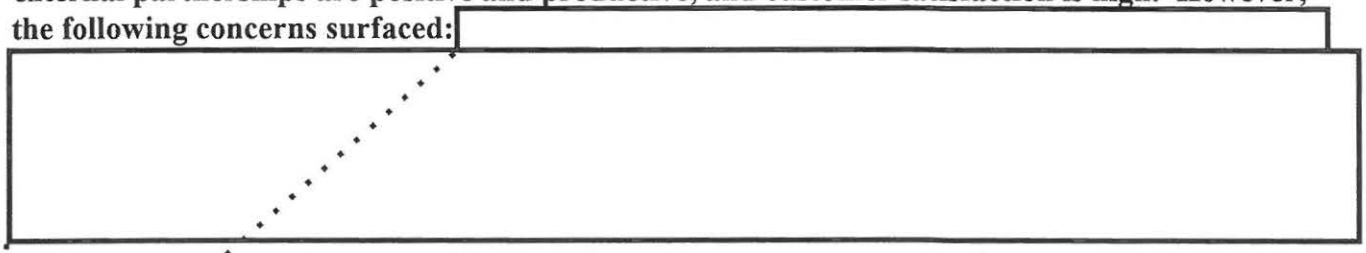
(U//~~FOUO~~) Management Action. **The Associate Directorate for Human Resource Services concurred with the report, with minor administrative changes.**

(U) Overall Report Classifications. **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U) Category. **Human Capital**

(U) China and Korea Missions; **NSA/CSS IG; IN-08-0001; 30 September 2008**

~~(S//REL)~~ Summary. **Our inspection of the China and Korea Production Center found that, with few exceptions, mission delegation and execution are working well, internal and external partnerships are positive and productive, and customer satisfaction is high. However, the following concerns surfaced:**



(U//~~FOUO~~) Management Action. **Management concurred with the recommendation and is taking corrective action.**

(b) (1)
(b) (3)-P.L. 86-36

(U) Overall Report Classifications. **TOP SECRET//COMINT//NOFORN**

(U) Category. **Joint Warfighting and Readiness**

(b) (6)

(U) Time & Attendance Fraud; NSA/CSS IG; IV-07-0029

(U//~~FOUO~~) Summary. **The OIG substantiated an allegation that, between March 2006 and March 2007, a GG-13 NSA employee intentionally submitted false and inaccurate timesheets for a total shortfall to the government of 786 hours. On [redacted] the employee pled guilty in United States District Court to a felony violation of Title 18, United States Code, Section 1001 (False Statements). On [redacted] the employee was sentenced to [redacted] years probation, [redacted] home confinement, and [redacted] hours community service. The court also ordered the employee to pay the government restitution in the amount of [redacted]**

(U) Management Action. **The employee resigned from the Agency in lieu of termination. In view of the criminal conviction, the matter was referred to the Associate Directorate for Security and Counterintelligence for security clearance action.**

(U) **Overall Report Classification. UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U) **Category. Other (Time and Attendance)**

(U) Procurement Fraud Initiative; NSA/CSS IG; Various Control Numbers; 1 April 2008 to 30 September 2008.

(U//~~FOUO~~) Summary. In October 2007, we launched an initiative to identify fraudulent billings by NSA/CSS contractors. This initiative involves the interrogation of contractor access data, coordination with company compliance officials, analysis of billing records, and the investigation of access and billing anomalies.

(U//~~FOUO~~) After twelve months, our initiative has produced significant results. To date, we have identified several hundred potential mischarging matters and completed more than 40 mischarging investigations. These investigations have revealed more than 9,000 hours charged by contractors for fraudulent billings or out-of-scope work. Recoveries for these hours will exceed $1.2 million. In most of the instances where fraud has been substantiatied, the company has terminated the offending employee. Some examples include:

(U//~~FOUO~~) IV-07-0055. A subcontractor employee fraudulently billed the government 298 hours (approximately $56,000) for non-work activities. The company reimbursed the government the full amount.

(U//~~FOUO~~) IV-07-0042. A subcontractor employee fraudulently billed 374 hours (approximately $39,000) for time spent at lunch. The company reimbursed the government for the full amount.

(U//~~FOUO~~) IV-08-0006. A contractor employee fraudulently billed 910 hours (approximately $68,000). The employee admitted to billing the government for time spent taking college courses.

(U//~~FOUO~~) IV-08-0014. A subcontractor employee admitted to billing 582 hours (approximately $98,000) for contract work performed at home, which was specifically prohibited under the contract terms. The contractor has offered $250,000 to settle all claims for out-of-scope work performed by its employees on that contract.

(U//~~FOUO~~) IV-08-0043. A contractor employee fraudulently billed 751 hours (approximately $82,000) for time spent taking care of personal matters during the workday.

The employee admitted to billing the government for personal matters.

(U) Special Inquiry: Employee Concerns – Yakima Research Station (YRS), WA; **NSA/CSS IG; ST-08-0023; September 2008**

(U//~~FOUO~~) Summary. **A spate of complaints from Yakima Research Stations (YRS) employees concerning work relationships prompted a quick reaction special study by the OIG. The study found that portions of the relatively small YRS workforce had become factionalized harming work relationships and creating discord. The new Chief of Station, YRS, who arrived only weeks prior to the OIG visit, has since restructured the site leadership team. This change appears to have substantially improved the situation. Additional recommendations regarding promotion administration and training for a specific work center were provided to the new Chief of Station.**

(U) Overall Report Classification. **SECRET//COMINT**

(U) Category. **Other (Intelligence Support/Standards of Conduct)**

(U) **OIG-Directed Management Inquiry: Hostile Work Environment Allegations – NSA/CSS Texas;** NSA/CSS IG; CO-08-0635; August 2008

(U//~~FOUO~~) **Summary.** The OIG tasked the NSA/CSS Texas command to conduct a management inquiry into actions by a mid-level manager who had been accused by several subordinates of hostile and abusive treatment. The management inquiry substantiated several instances during which the manager used abusive or profane language. The report has been forwarded to the NSA Office of Employee Relations for appropriate action.

(U) **Overall Report Classification.** U//FOUO

(U) **Category.** Other (Intelligence Support/Standards of Conduct)

(U) **Misuse of Government Resources**; NSA/CSS IG; CO-08-0384, CO-08-0403, CO-08-0453, CO-08-0454, CO-08-0455, CO-08-0517, CO-08-0525, CO-08-0526, CO-08-0563, CO-08-0673, CO-08-0674, CO-08-0723, CO-08-0724, CO-08-0771, CO-08-0791, 1 April 2008 to 24 September 2008.

(U//~~FOUO~~) **Summary.** The OIG substantiated 15 allegations of NSA affiliates' misuse of government resources (e.g., accessing adult-oriented material through the Agency's unclassified Internet network).

(U) **Management Action.** Subjects in these cases were civilian employees, military affiliates, and NSA contractor employees. Discipline ranged from a letter of warning to reduction in grade.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Computer Misuse)

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U//~~FOUO~~) **Advisory Report on Decompartmentation Plans for Counterterrorism Special Programs**; NSA/CSS IG; ST-08-0018; 30 June 2008

(U//~~FOUO~~) Summary. Our advisory report found that the Program Management Office (PMO) was diligent and thorough in assessing the scope and complexity of removing data from the compartmented program while ensuring compliance with laws, regulations, and other mandates. The content, communication, and assignment of supporting plans were adequate to provide reasonable assurance of compliance and successful implementation. Although a solid foundation of planning was in place, supporting plans need fine tuning. We made no formal recommendations;however, management should consider the need for more detailed written plans and firm milestones in the areas of document preservation, reporting, and debriefing. Most importantly, because the Program Management Office has formally disbanded, former PMO members and NSA leadership must rigorously monitor remaining actions to ensure that the decompartmentation is successful.

(U) Overall Report Classification. **TOP SECRET//COMINT//NOFORN**

(U) Category. Joint Warfighting and Readiness

(b) (3)-P.L. 86-36

(U) [redacted]

NSA/CSS IG; [redacted]

~~(S//REL)~~ **Summary. The objectives of this inquiry were to identify authorities for the handling of data in [redacted] and to determine if policies and procedures are in place and followed to ensure compliance with those authorities. We also reviewed system security practices for [redacted] Information Systems. Our special study found that overall the Associate Directorate for Security and Counterintelligence (ADS&CI) [redacted] is compliant with NSA's authorities. [redacted] ADS&CI obtained required approvals for [redacted] certified and accredited by the Technology Directorate. ADS&CI management has minimized risk by limiting access to [redacted] data, reviewing queries of the data, and providing review results to the Office of General Counsel. Although ADS&CI management has established a good control environment, some [redacted] information systems improvements are needed, and the Technology Directorate must improve oversight of [redacted] system security practices.**

(U//~~FOUO~~) **Management Action. ADS&CI management concurred with our findings Their planned actions, which will further reduce the risk associated with [redacted] operations, meet the intent of our recommendations.**

(U) Overall Report Classifications. **SECRET//REL TO USA, FVEY**

(U) Category. Joint Warfighting and Readiness

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

~~SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

(b) (1)
(b) (3)-P.L. 86-36

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) *For the Period October 1, 2006 Through March 31, 2007*

(~~S//REL~~) NSA/CSS IG (all three reports)

(~~S//REL~~) **Summary.** We visited three sites selected on the basis of risk, location, and reported oversight issues. Our reviews assessed site operations, local customer support activities, and compliance with intelligence oversight requirements and Based on our findings, management agreed to oversee and clarify local tasking procedures; clarify and enforce the requirement that all sites conduct emergency destruction drills; and to provide safety training for personnel

(U) **Overall Report Classifications.** TOP SECRET//COMINT (all three reports)

(U) **Category.** Joint Warfighting and Readiness

(b) (3)-P.L. 86-36

(U) **Special United States Liaison Officer Canberra, Australia**; NSA/CSS IG; IN-06-0008; 16 October 2006

(U//~~FOUO~~) **Summary.** Our inspection of the Special U. S. Liaison Officer Canberra (SUSLOC) found that he and his team are effectively representing the Director, National Security Agency/Chief, Central Security Service (NSA/CSS) and the Agency. They have the confidence of their counterparts in the Australian and New Zealand Signals Intelligence (SIGINT) organizations

(U) **Management Action.** Management concurred with all recommendations; corrective actions are underway.

(U) **Overall Report Classification.** TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category**. Joint Warfighting and Readiness

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(U) **Data Handling Controls Over a Sensitive SIGINT Database;** NSA/CSS IG; ST-06-0019; 17 October 2006 (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Summary.** The NSA/CSS Office of the Inspector General (NSA OIG) conducted a special study to follow up on a [redacted] of Inspector General's [redacted] OIG) inquiry on a data handling incident. The incident [redacted]

(U) **Management Action.** Management concurred with our findings and agreed to take corrective action.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category:** Joint Warfighting and Readiness

(U) **Information Warfare Support Center**; NSA/CSS IG; IN-06-0001; 19 October 2006

(U//~~FOUO~~) **Summary.** The Information Warfare Support Center (IWSC) brokers the SIGINT aspects of the information operations (IO) needs of the combatant commands with NSA/CSS and other Department of Defense, Intelligence Community, and government organizations. Our inspection found that, while IWSC customers are generally complimentary about the support they receive, many are confused by the emergence and continuing evolution of other NSA/CSS organizations engaged in various aspects of IO. In addition, loss of personnel and funding issues make it increasingly difficult for the IWSC to provide the level of service customers seek. The inspection determined that maintaining the organizational status quo is not the best course of action. We also found that: 1) customer representatives and internal partners do not understand the IWSC's roles and responsibilities and its relationship with the Joint Functional Component Command for Network Warfare and the NSA/CSS Threat Operations Center; 2) NSA cannot accurately track personnel on Joint Duty Assignment billets and; 3) the IWSC has not corrected five findings from a Communications Security audit in 2003, that, combined with two incidents in 2005, indicate a serious problem that requires urgent attention.

(U) **Management Action.** Management concurred on all recommendations and is taking corrective action.

(U) **Overall Report Classification**. TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category**. Joint Warfighting and Readiness

(b) (1)
(b) (3)-P.L. 86-36

(U) **Directorate of Engineering**; NSA/CSS IG; IN-06-0011; 6 November 2006

(~~S//REL~~) **Summary.** Our organizational inspection of the Directorate of Engineering (DE) found that, despite significant progress in recognizing that Systems Engineering (SE) and enterprise architecture are critical to transformation activities, the Agency still has not completed an operational capabilities baseline

(U) **Management Action.** The Director for Business Management and Integration and the Chief Systems Engineer are already acting on our recommendations.

(U) **Overall Report Classification.** SECRET//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(U) **NSA/CSS Texas**; NSA/CSS IG, INSCOM IG, AIA IG, NNWC IG; JT-06-0004; 5 December 2006

(b) (3)-P.L. 86-36

(~~U//FOUO~~) **Summary.** The IG organizations of the U.S. Army's Intelligence and Security Command (INSCOM), Air Intelligence Agency (AIA), Naval Network Warfare Command (NNWC), and NSA conducted a joint inspection of NSA/CSS Texas (NSAT) in August 2006. The team found that NSAT is struggling to transform and grow its missions in accordance with the Mission Alignment and Cryptologic Center Build-out, despite cuts in the resources needed to support such growth.

(U) **Management Action.** Management concurred with the findings of the joint inspection team and is taking corrective action.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(U//~~FOUO~~) **Inspector General Reviews That Indicate Major Systemic Issues;** NSA/CSS IG; ST-07-0012; 21 December 2006

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Summary.** At the request of the Deputy Chief of Staff, the Office of the Inspector General identified reviews that it completed from 2000 to the present that indicated major systemic issues at NSA. The OIG assigned the following [ ] categories to these reviews: [ ]

[ ]

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Joint Warfighting and Readiness

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) **Satellite Modernization Program**; NSA/CSS IG; AU-06-0007A; 21 December 2006

(~~S//REL~~) **Summary.** An audit of [ ] detected an issue that

[ ]

(U) **Management Action.** Given the competing priorities for funds within the Agency, the Signals Intelligence Directorate will decide, based on a new life cycle cost estimate, whether to pursue different alternatives for this important modernization program.

(U) **Overall Report Classification.** TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category**. Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Access to** [ ] NSA/CSS IG; [ ]

(U//~~FOUO~~) **Summary.** Our special study found that NSA is [ ]

[ ]

(b) (3)-P.L. 86-36

(U) **Management Action.** Management concurred with all recommendations and corrective actions are being taken.

(U) **Overall Report Classification.** SECRET//COMINT//TALENT KEYHOLE//REL TO USA, AUS, GBR

(U) **Category.** Joint Warfighting and Readiness

(U) **NSA/CSS Georgia;** NSA/CSS IG, INSCOM IG, AIA IG, NNWC IG; JT-07-0001; 5 February 2007

(U~~//FOUO~~) **Summary.** The joint inspection team conducted an inspection of NSA/CSS Georgia (NSAG) and found that the importance of the NSAG mission, which directly supports the Global War on Terror, is a great motivator for the entire workforce. Civilian and military leaders have forged good working relationships. Nonetheless, fissures are apparent, related to confusion arising from governance issues and the "pause" in resourcing Mission Build-Out. The near-term viability of some of the new missions should be reassessed in light of the "pause," which is affecting morale, particularly for assignees sent to stand up new missions. need to work with Global Capabilities Managers at NSA, Washington (NSAW), to clearly define the division of effort between NSAG and NSAW target offices. Absent formal guidelines on the "Run Rich" approach to hiring, we found instances where as many as people were assigned to a single billet.

(U) **Management Action.** Management concurred with the findings of the joint inspection team and is taking corrective action.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness (b) (3)-P.L. 86-36

(U) **Electronic Funds Transfer**; NSA/CSS IG; AU-06-0019; 20 February 2007

(U~~//FOUO~~) **Summary.** The Agency has not fully complied with the law (in effect since 1998) that requires the use of electronic fund transfer (EFT) for virtually all disbursements. After the theft of U.S. Treasury checks worth about the NSA Comptroller launched an effort to increase the use of EFT for accounts payable transactions; EFT for these payments rose in April 2006 to in September 2006. The Agency has achieved good compliance in two areas – payroll (about 99 percent) and travel (about 94 percent) of FY2006 transactions – but still falls short of the law's intent, particularly in the area of accounts payable. We found two

principal reasons why checks are still issued for about [redacted] transactions that, by law, should be processed electronically: the Agency's current financial systems are unable to handle [redacted] processes needed for EFT and the Accounting and Financial Services organization has no overall process to identify and document the justification for those recipients who are paid by check.

(U) **Management Action.** The Directorate of Finance concurred with two recommendations and is working with the [redacted] Office to implement the third.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Financial Management

(b) (3)-P.L. 86-36

(U) **Communications Security Accountability Program;** NSA/CSS IG, AU-06-0004; 2 March 2007

(U~~//FOUO)~~ **Summary.** The audit found that the Agency cannot account for all of the Communications Security (COMSEC) material assigned to its Central Office of Record. For example, [redacted] COMSEC items in the [redacted] accounts we sampled were missing. This lack of accountability is a direct result of the antiquated and labor-intensive process used to account for COMSEC items. [redacted] is very inefficient and prone to errors. Moreover, when government (military and civilian) users reported lost COMSEC material, there was no independent investigation to determine the cause. We also found that many COMSEC audits and semiannual inventories were overdue; [redacted]

(U) **Management Action.** Management officials agreed to act on our recommendations to resolve the internal control weaknesses within the COMSEC accounting program.

(U) **Overall Report Classification.** SECRET//NOFORN

(U) **Category.** Joint Warfighting and Readiness

(U) **Electrical Power Consumption at NSA;** NSA/CSS IG, AU-07-0004; 6 March 2007

(~~C//REL~~) **Summary.** [redacted]

(b) (1)
(b) (3)-P.L. 86-36

[redacted]

(U) **Management Action.** Management agreed to implement our recommendations.

(U) **Overall Report Classification.** TOP SECRET//COMINT//TALENT KEYHOLE//NOFORN

(U) **Category.** Other (b)(3)-P.L. 86-36

(U) **Leased Facilities Planning and Fit-up;** NSA/CSS IG, AU-06-0020; 16 March 2007

(~~C//REL~~) **Summary.** The audit followed up on an allegation regarding problems that delayed occupancy of the new building to house the [redacted] Problems in fitting up two leased facilities, including the [redacted] revealed serious flaws in project oversight by the Facilities Services organization. Long delays and an incomplete communications infrastructure increased the cost of activities conducted at the [redacted] The Agency paid lease costs of about [redacted] Most of these problems can be traced to the lack of comprehensive project management with clear lines of authority.

(U) **Management Action.** The Office of Facilities Services, Office of Physical Security, the Information Technology Directorate, and the Information Assurance Directorate concurred with our recommendations and have already begun corrective action.

(U) **Overall Report Classification.** SECRET//COMINT//NOFORN

(U) **Category.** Joint Warfighting and Readiness (b)(1) (b)(3)-P.L. 86-36

(U) **NSA's Secure Cellular Phone Program;** NSA/CSS IG, ST-06-0010; 22 March 2007

(~~S//REL~~) **Summary.** The Agency purchased over [redacted] secure cell phones, primarily due to Congressional earmarks. Our special study found that,

[redacted]

(~~S//REL~~) **Management Action.** IAD agreed to implement our recommendations

[redacted]

(b) (1)
(b) (3)-P.L. 86-36

[redacted] appears to be the most cost-effective solution at this time.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Joint Warfighting and Readiness

(U) **Office of the Middle East and North Africa**; NSA/CSS IG;IN-06-0006; 30 March 2007

(U//~~FOUO~~) **Summary**. The Middle East & North Africa Office (MENA) produces Signals Intelligence (SIGINT) to satisfy information needs (INs) of combatant commands and other Department of Defense (DoD), Intelligence Community (IC), and government organizations pertaining to MENA's targets of primary concern. Our organizational inspection found that MENA customers are generally complimentary about the support they receive, and MENA partners reported having a professional, collaborative working relationship with MENA Office personnel. However, MENA's SIGINT Development (SIGDEV) Division is not centrally managing all MENA SIGDEV activities to optimize collaboration and weigh the trade-offs between day-to-day production and future target development. [redacted]

(U) **Management Action.** Management concurred with all recommendations and has already begun taking corrective action.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(b) (3)-P.L. 86-36

(U) **Human Resources Information Technology Modernization**; NSA/CSS IG; IN-06-0004; 30 March 2007

(U//~~FOUO~~) **Summary**. Various types of human resource (HR) data about Agency affiliates is scattered in directories and databases – [redacted] – throughout the Enterprise. This longstanding problem means that decision makers at NSA Headquarters cannot get all the HR information they need when they need it. The proposed solution, [redacted]

(U) **Management Action.** Management concurred with all recommendations; however, resolution will require leadership from the highest levels of management.

(U) **Overall Report Classification.** SECRET//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Human Capital

(U) **Labor Mischarging**; NSA/CSS IG; IV-06-0059; 26 October 2006

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a contract employee mischarged 105.90 labor hours while working on NSA contracts during the 2005 – 2006 timeframe. This amounted to approximately $21,211 in charges falsely billed against NSA contracts. The contractor reimbursed NSA that amount. The employee had resigned from the company prior to the start of our investigation. The U.S. Attorney's Office, District of Maryland, declined prosecution due to the contractor's cooperation and reimbursement to NSA.

(U) **Management Action.** Company made restitution in accordance with our findings.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Contract Fraud)

(U) **Labor Mischarging**; NSA/CSS IG; IV-06-0060; 20 November 2006

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a contract employee mischarged 344.5 labor hours while working on NSA contracts during the 2005 - 2006 timeframe. This amounted to approximately $50,065 in charges falsely billed against NSA contracts. The contractor reimbursed NSA that amount. The U.S. Attorney's Office, District of Maryland, declined prosecution due to the contractor's cooperation and reimbursement to NSA.

(U) **Management Action.** Company made restitution in accordance with our findings.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Contract Fraud)

(U) **Labor Mischarging;** NSA/CSS IG; IV-06-0061; 23 February 2007

(U//~~FOUO~~) **Summary.** The OIG substantiated an allegation that a contract employee mischarged NSA contracts during the 2005 - 2006 timeframe. This amounted to approximately $10,000 in charges falsely billed against NSA contracts. The contractor reimbursed NSA that amount and the employee no longer holds a clearance to work on Agency contracts. The U.S. Attorney's Office, District of Maryland, declined prosecution due to the contractor's cooperation and reimbursement to NSA.

(U) **Management Action.** Company made restitution in accordance with our findings.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category**. Other (Contract Fraud)

(U) **Time and Attendance Investigations**; NSA/CSS IG; IV-06-0038 (13 Oct 06); IV-06-0040 (18 Oct 2006); IV-06-0049 (14 Mar 2007); IV-06-0055 (30 Nov 2006); IV-06-0063 (1 Dec 2006); IV-07-0005 (19 Mar 2007); IV-07-0006 (12 Mar 2007)

(U~~//FOUO~~) **Summary.** The OIG substantiated seven allegations of Time and Attendance abuse, wherein employees claimed over 3,037 hours in excess of those they were determined to have actually worked. In the aggregate, these cases will result in the recovery of approximately $108,300 in funds paid to employees for hours falsely claimed.

(U~~//FOUO~~) **Management Action.** Administrative recoupment action will recover the $108,300 mischarged to the agency, and the responsible employees were referred for additional administrative disclipinary action.

(U) **Overall Report Classifications.** UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

(U) **Category.** Other (Fraud)

(U) **Diploma Mill Degree;** NSA/CSS IG; IV-06-0053, 7 March 2007

(U) **Summary.** The OIG received information that an Agency employee may have received his Bachelor of Arts degree from a "diploma mill." Our investigation concluded that the employee deliberately misrepresented his credentials and qualifications to NSA when he claimed a Bachelor of Arts degree from a non-accredited institution.

(U) **Management Action.** This matter was referred to NSA Employee Relations for disciplinary action.

(U) **Overall Report Classification**. UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Waste of Resources)

(U) **Procurement Fraud/Criminal Conflict of Interest – Felony Conviction;** NSA/CSS IG; IV-05-0038 (b) (6)

(U) **Summary**. As the result of an 18-month NSA OIG investigation, a former GG-14 NSA employee within IAD pled guilty [redacted] to a felony violation of the Federal criminal conflict of interest statute, 18 U.S.C. § 208. [redacted] he was sentenced to two years probation, six months home confinement, 50 hours community service, and a $100,000 fine (payable in 15 days). During his employment with NSA, this individual co-created and directed the [redacted] At the same time he was [redacted] as an NSA employee, companies owned by him and/or his spouse obtained [redacted] support-related government contracts or subcontracts totaling over $750,000. As a result of the NSA OIG investigation, the government cancelled as unnecessary an ongoing $300,000 contract in support of the 2006 [redacted] thereby allowing funds to be put to better use. Further, NSA determined that, in the future, similar

contracted support to the [redacted] would not be required, resulting in a potential cost avoidance to the government of $1.5 million over the next 5 years. NSA is currently pursuing the debarment of both the former employee and the companies involved.

(U) **Overall Report Classification**. UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Acquisition Processes and Contract Management

(U) **Waste of Agency Resources**; NSA/CSS IG; IV-06-0054; 1 December 2006

(U) **Summary.** This investigation was conducted in response to an allegation that an Agency employee received tuition assistance of $22,773 from the Agency in furtherance of a Doctoral degree from the [redacted] but never completed any of the necessary scholastic work for this degree. We substianted the allegation and concluded that the employee caused the Government to waste eight semesters' worth of tuition payments.

(U) **Management Action.** This matter has been referred for administrative action and recoupment of the funds from the employee.

(U) **Overall Report Classification**. UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Waste of Resources)

(b) (6)

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) Ongoing

(U) **Inspection of SID's Chemical, Biological, Radiological, Nuclear Mission**; NSA/CSS IG; IN-06-0002

~~(S//REL)~~ **Background.** Chemical, Biological, Radiological, and Nuclear (CBRN) terrorism is one of the most menacing threats to U.S. security, and from a Signals Intelligence (SIGINT) perspective, [redacted] work the CBRN target from varying perspectives. The inspection is evaluating CBRN mission performance, including examining the execution of CBRN as a transnational target, assessing the impact of Mission Build-Out, and reviewing any funding or human resource issues.

(U) **Inspection of the Geospatial Exploitation Office**; NSA/CSS IG; IN-06-0005

(U~~//FOUO~~) **Background** The Geospatial Exploitation Office (GEO) began operations in [redacted] GEO's primary objective will be to assess GEO's mission effectiveness and their ability to satisfy requirements and information needs levied on the organization. The inspection will determine whether the current organization's missions and functions are being properly executed in an efficient and effective manner; whether missions and functions are accurately portrayed and being accomplished; establish whether missions performed are appropriately placed within the product line; and will identify any impediments, which hinder the efficient and effective execution of their missions and functions.

(b)(3)-P.L. 86-36

(U) **Special Studies of Counterterrorism Programs**; NSA/CSS IG

(U~~//FOUO~~) **Background:** While the NSA Counterterrorism Special Programs were being conducted under Presidential authority, the OIG performed continuous audits. The overall objectives were to determine whether there were appropriate policies and procedures in place for activities under the program consistent with the terms of the Presidential Authorization; to evaluate their efficiency and effectiveness in mitigating any

high-risk activities associated with the program; and to identify any impediments to satisfying the requirements of the Presidential Authorization. In January 2007, all of these programs began operating under the authority of Foreign Intelligence Surveillance Court orders. For these new orders, the OIG is performing reviews in accordance with their terms, which specify that an initial review will be done to ensure that minimization procedures are adequate.

(U) Planned

(U) Assistance to ODNI IG for the Terrorist Watchlist Project; NSA/CSS IG; JT-07-0006

(U) **Background.** The Terrorist Screening Center (TSC) maintains a consolidated terrorism watchlist that is populated by information from the National Counterterrorism Center (NCTC) and the Federal Bureau of Investigation (FBI). Agencies that possess or acquire terrorism and counterterrorism information, with the exception of purely domestic counterterrorism information, are required by Executive Order 13354 to promptly give access to such information to the NCTC. The NCTC provides a subset of that information to the TSC for inclusion on the consolidated watchlist. The Intelligence Community Inspectors General (ICIG) Forum agreed to coordinate a review of the processes for nominating individuals to the consolidated terrorist watchlist. The Offices of the Inspector General of the Office of the Director for National Intelligence (ODNI), Central Intelligence Agency (CIA), Department of Justice (DOJ), Defense Intelligence Agency (DIA), National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), Department of State (State), and Department of Treasury (Treasury) will participate in the joint review.

(U) **Advisory Report Associated with Expeditionary SIGINT Deployments To Hostile Areas**; NSA/CSS IG; ST-07-0015

(U~~//FOUO~~) **Background.** During 2005, the IG conducted research into Agency activities associated with Expeditionary SIGINT Deployments to hostile areas. The resultant report (ST-06-0001 – *Advisory Report on the Activities Associated with Expeditionary SIGINT Deployments to Hostile areas*) surfaced issues related to the candidate selection process, pre-deployment operations training, and corporate resolution of issues raised in after-action reports. The report also emphasized the need for appropriate IT support. The follow-up review will: a) determine if issues raised in the earlier report have been adequately addressed; b) assess the effectiveness of the changes/improvements that have been implemented; and c) surface any new issues.

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) ***For the Period April 1, 2006 Through September 30, 2006***

(U) **Office of Physical Security's Practices Relative to Protest Activity**; NSA/CSS IG; ST-06-0012; 28 April 2006

(U//~~FOUO~~) **Summary.** An article published in *The Sun* on 13 January 2006 alleged that NSA monitored members of the Baltimore Pledge of Resistance, a peace group tied to the Baltimore Emergency Response Network, as they prepared to protest at Fort Meade. The article also alleged that NSA used law enforcement agencies to track the activists. We conducted this special study to (a) identify the NSA Police authorities relative to the activities of protesters on or near NSA property; (b) determine if policies and procedures were in place to ensure compliance with those authorities; and (c) determine if the policies and procedures were followed on 3 July 2004 during protests at NSA by the Baltimore Pledge of Resistance peace group. We found that NSA Police were authorized, pursuant to Section 11 of Public Law 86-36, to protect buildings, grounds, and property solely under the administration and control of, and used extensively by NSA. We also concluded that NSA police acted in accordance with applicable authorities, policies, and procedures while performing duties associated with the protest activity. Finally, the Agency made no attempt to use the Signals Intelligence system to monitor this protest activity.

(U) **Overall Report Classification.** CONFIDENTIAL//REL to USA, AUS, CAN, GBR, NZL

(U) **Category.** Homeland Defense

(U) **Time Synchronization Issue**; NSA/CSS IG; ST-06-0013; 19 May 2006

~~(S)~~ **Summary.** One of the many challenges the Agency faces when analyzing complex signals is the accurate measurement and retention of time-related information. To accomplish its various missions, NSA must reliably affix accurate time date stamps and, when available, geolocation information on all collected signals. After receiving reliable indications that NSA's ability to affix and retain accurate time measurement is deficient, the OIG announced its intention to begin a special study of this subject. In response to similar indications, the Director, NSA announced the creation of the Time and Frequency Coordination Authority (TFCA or Authority) in May 2006. As a result, we curtailed the special study to give the TFCA a chance to address the deficiencies we have reason to believe exist. We will therefore make periodic inquiries into TFCA's progress in the coming months.

(U) **Overall Report Classification.** TOP SECRET//COMINT

(U) **Category.** Joint Warfighting and Readiness

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~20291123~~

(U) **Oversight Review of Restaurant Fund, CWF, and Gift Shop**; NSA/CSS IG; AU-06-0015; 2 June 2006

(U//~~FOUO~~) **Summary.** A firm of Certified Public Accountants (CPAs) issued unqualified opinions on the reliability of the financial statements of the Agency's Restaurant Fund, Civilian Welfare Fund, and the Cryptologic Museum Gift Shop. Our oversight review of the CPA audit found no problems in the conduct of the recent audit by the CPA firm but identified two concerns: high-speed internet connection and nonappropriated fund instrumentality (NAFI) contract. Without a connection to high-speed internet service, the NAFI's business and accounting services will continue to be highly inefficient. The current NAFI contract (and all option years) for the contract with the CPA firm that reviews Agency NAFIs has expired. A new competitive effort needs to be awarded and in place before 30 September 2006 so that the contracted CPAs can be on hand to observe the ending inventory.

(U) **Management Action.** Management concurred with and is implementing our recommendations.

(U) **Overall Report Classification**. UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category**. Financial Management

(U) **Award Fee Contracts**; NSA/CSS IG; AU-06-0002; 30 June 2006

(U//~~FOUO~~) **Summary.** As of 1 October 2005, NSA had award fees on [redacted] contracts valued at over [redacted]. Our audit reviewed [redacted] award fee contracts valued at [redacted] with total available award fees of [redacted] about 78 percent or [redacted] of the award fees were paid out. We concluded that the Agency needs a consistent approach to these contracts so award fees achieve their purpose: to help control program risk and improve contractor performance. The Agency's ability to evaluate contractor performance is impeded by (1) failure to document a basis for the award fee percentage; (2) award fee plans that do not allow for meaningful ratings (3) inconsistent evaluation methodologies; and (4) the absence of formal training in how to administer award fee contracts. We also question the use of Time & Material-Award Fee contracts because they place a heavy administrative burden on the Agency and do not emphasize acquisition outcomes.

(U) **Management Action.** Management concurred with all recommendations; corrective actions are underway.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category**. Acquisition Processes and Contract Management (b) (3)-P.L. 86-36

(U) **Military Interdepartmental Purchase Requests and Economy Act Orders**; NSA/CSS IG; AU-05-0008; 12 July 2006

(U//~~FOUO~~) **Summary.** Over the last 2 fiscal years, Military Interdepartmental Purchase Requests (MIPRs) and Economy Act Orders (EAOs) represented [redacted] and [redacted] percent, respectively, of the total funds (over [redacted] for each year) used to purchase goods and services for NSA. Our audit found that the current practice of delegating the authority to approve MIPRs/EAOs to Senior Executives or Flag Officers is not achieving the

(b)(3)-P.L. 86-36

intent of the law; MIPRs/EAOs are not reviewed by a Contracting Officer or an independent entity to see if there is a valid reason for bypassing the Contracting Group; and the originating offices at NSA did little to monitor the billing and accounting for MIPRs and EAOs and did not always verify that goods and services were delivered.

(U//~~FOUO~~) **Management Action.** Management concurred with our recommendation to update the draft policies to strengthen internal controls over MIPRs/EAOs but nonconcurred with the recommendation to establish a separate Agency oversight mechanism. This was resolved when management agreed that the Acquisition Program Managers will now be responsible for oversight of MIPRs and EAOs.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Acquisition Processes and Contract Management

~~(S)~~ [redacted] NSA/CSS IG; [redacted]

~~(S)~~ **Summary.** Our special study on [redacted] found the Cryptanalysis and Exploitation Services (CES) organization to be control conscious, with many strong management controls in place to ensure the integrity of [redacted] CES can further improve internal controls over [redacted] provided the procedures for handling [redacted] are formally reissued, properly coordinated, and fully address the procedural and compliance issues cited in our report.

(b)(1)
(b)(3)-P.L. 86-36

(U) **Management Action.** Management concurred in our findings and recommendation, agreed to take corrective actions, and plan to complete all actions by 31 December 2006.

(U) **Overall Report Classification.** TOP SECRET//COMINT/NOFORN

(U) **Category.** Joint Warfighting and Readiness

(U) **Followup Report on the** [redacted] NSA/CSS IG; [redacted] 21 July 2006

~~(S)~~ **Summary.** Since 2003, the Agency [redacted] at NSA/CSS Hawaii. [redacted] initiatives were the subject of a finding and recommendation in the February 2005 Joint IG report at Hawaii. We closed the recommendation to address key policy shortfalls based on actions planned by the Directorate of Engineering (DE) and Corporate Planning. During a followup inspection, we found that [redacted] and DE and Corporate Planning have not issued two policies that address deficiencies noted in the 2005 Joint IG Report.

~~(S)~~ **Management Action.** Management decided to withdraw the FY2006 funds [redacted] and agreed to complete the relevant policy documents by January 2007.

(U) **Overall Report Classification.** TOP SECRET//COMINT//TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, NZL

(b)(1)
(b)(3)-P.L. 86-36

(U) **Category.** Joint Warfighting and Readiness (b) (3)-P.L. 86-36

(U) **FY2006 Report on Compliance with the Federal Information Security Management Act at NSA/CSS**; NSA/CSS IG; AU-06-0009; 31 July 2006

(U//~~FOUO~~) **Summary.** NSA is making a concerted effort to address the weaknesses identified in our FY2005 audit of compliance with *The Federal Information Security Management Act* (FISMA). Despite continuing impediments, the Agency's Chief Information Office (CIO) made progress in carrying out the Plan of Action and Milestone to address the certification and accreditation (C&A) of Agency systems – identified as a material weakness in FY2002. By June 2006, about [redacted] of all Agency systems and [redacted] of mission-critical systems (compared to [redacted] a year ago) were fully accredited. Our FY2006 FISMA review found weaknesses from prior years that were not fully mitigated: [redacted]

(U) **Management Action.** The CIO continues to make progress in addressing FISMA requirements. This includes holding bi-weekly meetings to track and report C&A progress and challenges for mission-critical systems. In addition, the Office of Information Assurance Services reviewed C&A data for accuracy, and the CIO engaged an outside firm to do a complete review of NSA's operational information security program. This resulted in [redacted] recommendations, which the CIO has used to baseline its budget for FY2007. This improved the CIO's ability to capture important IT security performance measures, as required by FISMA legislation.

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Information Technology Management

(U) **Alaska Mission Operations Center;** NSA/CSS IG, AIA IG; NNWC IG; JT-06-0002; 4 August 2006

~~(S)~~ **Summary.** A joint team of inspectors from the Air Intelligence Agency (AIA), Naval Network Warfare Command (NNWC), and NSA Inspectors General conducted the first joint inspection of the Alaska Mission Operations Center (AMOC). Although the AMOC was officially 2 years old at the time of this inspection, we found no Concept of Operations or Implementation Plan for establishing the Center. Although progress is being made in attaining the presumed intent for the AMOC, progress is impeded by the lack of clearly defined authorities, responsibilities, processes, and chains of command. We also found that the Intelligence Oversight program needs many adjustments– some major and some minor, and Mission Operations was in transition, taking on new missions from other sites and working to expand [redacted] Overall, communications and computer systems and Network operations were well managed, but [redacted]

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(b) (1)
(b) (3)-P.L. 86-36

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

(U) **Category.** Joint Warfighting and Readiness

(U) **Asset Management and Cost Allocation for GROUNDBREAKER Contract;** NSA/CSS IG; AU-06-0001; 18 September 2006

(U//~~FOUO~~) **Summary.** The GROUNDBREAKER (GB) contract supports the Agency's non-mission Information Technology (IT) infrastructure. Each month GB bills the Agency for basic services in four service areas: Distributed Computing, Networks, Telephony, and Enterprise Management. Our audit recommendations focused on improving asset management, personnel data, and other areas. In asset management, we found process deficiencies in physical inventories and discrepancies in inventory data that contributed to a [redacted] percent inventory record error. Based on the results of our random statistical sample for October 2005, we projected the Agency may have been over billed by $346,630. Regarding personnel data, [redacted] Based on this process, our sample indicated a potential over payment of about $126,000 for October 2005.

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(U) **Overall Report Classification.** CONFIDENTIAL//PROPIN (b)(3)-P.L. 86-36

(U) **Category.** Acquisition Processes and Contract Management

(U//~~FOUO~~) **Joint Defense Facility Pine Gap;** NSA/CSS IG, AIA IG; NNWC IG, INSCOM IG; JT-06-0003; 21 September 2006

~~(C)~~ **Summary.** A joint team of inspectors from the the Air Intelligence Agency (AIA), Naval Network Warfare Command (NNWC), Intelligence and Security Command and NSA Inspectors General conducted a joint inspection of the Joint Defense Facility Pine Gap (JDFPG). We found a very strong mission focus at the site. However, two problems that impede mission operations require immediate attention from senior leadership:

[redacted]

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(U) **Overall Report Classification.** TOP SECRET//COMINT//TALENT KEYHOLE//REL TO USA, AUS, GBR

(b)(1)
(b)(3)-P.L. 86-36

(U) **Category.** Joint Warfighting and Readiness

(U) **NSA's Ability to Detect, Contain, and Recover from Computer Security Incidents;** NSA/CSS IG; AU-05-011B; 26 September 2006

(U//~~FOUO~~) **Summary.** The audit objective was to determine if NSA/CSS has effective and efficient internal controls to prevent, detect, analyze, contain, and recover from computer security incidents affecting the NSA/CSS computing environment. Our findings corroborate the Chief Information Officer's assessment that

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(b) (3)-P.L. 86-36

(U) **Overall Report Classification.** TOP SECRET//COMINT//NOFORN

(U) **Category.** Information Technology Management

(U) **Corporate Communications Strategy Group**; NSA/CSS IG; IN-05-0003; 27 September 2006

(b) (1)
(b) (3)-P.L. 86-36

~~(C)~~ **Summary.** Our organizational inspection found that the Agency's communications and multimedia activities have not been centralized in the Corporate Communications Strategy Group. As seen in OIG reviews of other corporate enablers, the mission organizations eventually regrow these functions, using mission funds and personnel, when corporate sponsors cannot provide support. For example, we found that the Corporate Communications Strategy Group is not aware of nor does it have oversight over Agency contracts—totaling about

(U) **Management Action.** Management concurred in all recommendations and corrective action is being taken.

(U) **Overall Report Classification.** SECRET//COMINT//REL TO USA, CAN, GBR, NZL

(U) **Category.** Information Technology Management

(U) **Time and Attendance Investigations**; NSA/CSS IG, IV-05-0034, 18 July 06; IV-06-0011,22 May 2006; IV-06-0013,12 September 2006; IV-06-0027, 15 August 2006; IV-06-0030, 7 September 2006; IV-06-0033, 20 Jun 2006; IV-06-0035, 4 August 2006; IV-06-0036, 29 June 2006; IV-06-0043, 20 June 2006; IV-06-0046, 15 September 2006; IV-06-0052, 26 September 2006

(U) **Summary.** The OIG substantiated eleven allegations of Time and Attendance fraud. In the aggregate, these cases will result in the administrative recoupment of approximately $93,000 in Government funds paid for duty hours falsely claimed.

(U) **Overall Report Classifications.** UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

(U) **Category.** Other (Fraud)

(U) **Labor Mischarging**; NSA/CSS IG; IV-06-0012;26 September 2006

(U~~//FOUO~~) **Summary.** The OIG substantiated an allegation that a contract employee mischarged 135 labor hours while working on NSA contracts during the 2003 – 2005 time period. This amounted to approximately $19,000 in charges falsely billed against NSA contracts, and the contractor reimbursed NSA that amount. The contractor also terminated the employee. The United States Attorney's Office, District of Maryland, declined prosecution due to the contractor's cooperation and reimbursement to NSA.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Fraud)

(U) **Labor Mischarging**; NSA/CSS IG; IV-06-0028; 26 September 2006)

(U~~//FOUO~~) **Summary.** The OIG substantiated an allegation that a contract employee mischarged 185 labor hours while working on NSA contracts in 2005. This amounted to approximately $36,300 in charges falsely billed against NSA contracts, and the prime contractor has agreed to reimburse the NSA by that amount. The prime contractor terminated the employee. The United States Attorney's Office, District of Maryland, declined prosecution due to the prime contractor's cooperation and reimbursement.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Fraud)

(U) **Falsification of an Official Document**; NSA/CSS IG; IV-06-0034; 21 July 2006

(U~~//FOUO~~) **Summary.** The OIG substantiated an allegation that a GG-13 NSA/CSS employee falsified the rating score on his 2005 Performance Review, forged management signatures, and submitted the document to the Agency in support of his 2006 promotion application. The matter was referred for disciplinary adjudication.

(U) **Overall Report Classification.** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category.** Other (Fraud)

(U) **Travel Voucher Fraud**; NSA/CSS IG; IV-06-0008;26 September 2006; IV-06-0009, 22 September 2006; IV-06-0024, 14 August 2006

(U~~//FOUO~~) **Summary.** The OIG substantiated three allegations of travel voucher fraud. Two investigations involved false travel expense report claims for Personally Operated Vehicle mileage by an NSA employee and an NSA military assignee. A third investigation involved an employee who repeatedly remained in country longer than necessary on OCONUS TDYs, and falsely claimed per diem on his travel vouchers. The Agency will recover a total of approximately $20,000 in Government funds as a result of these three investigations.

(U) **Overall Report Classifications.** UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

(U) **Category.** Other (Fraud)

(U) **Misuse of Government Resources;** NSA/CSS IG; IV-06-0023;14 June 2006

(U~~//FOUO~~) **Summary.** The OIG's Offices of Intelligence Oversight and Investigations conducted a joint inquiry into an allegation that an NSA/CSS employee violated applicable law and regulation by using Government property for unauthorized and unofficial purposes. The inquiry substantiated the misuse allegation and the matter was referred to the NSA OGC for consideration of referral to the Department of Justice.

(U) **Overall Report Classification.** TOP SECRET//COMINT

(U) **Category.** Other (Misuse of Resources)

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(b) (1)
(b) (3)-P.L. 86-36

(U) Ongoing

(U//~~FOUO~~) **Inspection of the Information Warfare Support Center**; NSA/CSS IG; IN-06-0001

~~(S)~~ **Background** The Information Warfare Support Center (IWSC) began operations in November 1994 in response to the need for SIGINT support to Information Operations (IO). IWSC's mission is to provide the combatant commander(s) with [redacted] related to counterterrorism. The primary objectives of this inspection include the following: a) determining whether the IWSC is executing its current missions and functions in an efficient and effective manner and in accordance with its charter, identifying any impediments to mission accomplishment; b) determining whether IWSC personnel comply with Internal Management Controls and other Agency regulations and policies governing personnel and organizational management; and c) assessing how well IWSC shares information with internal and external customers.

(U) **Inspection of SID's Chemical, Biological, Radiological, Nuclear Mission**; NSA/CSS IG; IN-06-0002

~~(S)~~ **Background.** Chemical, Biological, Radiological, and Nuclear (CBRN) terrorism is one of the most menacing threats to U.S. security, and from a Signals Intelligence (SIGINT) perspective, [redacted] work the CBRN target from varying perspectives. The inspection is evaluating CBRN mission performance, including examining the execution of CBRN as a transnational target, assessing the impact of Mission Build-Out, and reviewing any funding or human resource issues.

(U) **Inspection of the Middle East and North Africa Product Line**; NSA/CSS IG; IN-06-0006

~~(S)~~ **Background**. The mission of the Signals Intelligence Directorate 's Deputy Directorate for Analysis and Production includes the countries located in the Middle East and North Africa (MENA). The Office of MENA creates analytic strategies, performs SIGINT development, and creates SIGINT products and services in response to customer Information Needs. It is also deeply involved in SIGINT production to support the Agency's counterterrorism activities. The primary objectives of the inspection include the following:

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

a) determine the effectiveness and efficiency in which the Middle East and North Africa Product Line organization is performing mission operations functions; b) identify impediments that the organization faces in SIGINT production; and c) determine whether the organization's personnel comply with Internal Management Controls and other Agency regulations and policies governing personnel and organizational management.

(U//~~FOUO~~) **Inspection of the Geospatial Exploitation Office**; NSA/CSS IG; IN-06-0005

~~(S)~~ **Background** The Geospatial Exploitation Office (GEO) began operations in [redacted] The primary objective will be to assess GEO's mission effectiveness and their ability to satisfy requirements and information needs levied on the organization. The inspection will determine whether the current organization's missions and functions are being properly executed in an efficient and effective manner; whether missions and functions are accurately portrayed and being accomplished; establish whether missions performed are appropriately placed within the product line; and will identify any impediments, which hinder the efficient and effective execution of their missions and functions.

(b) (1)
(b) (3)-P.L. 86-36

~~(S)~~ [redacted] **Regional Review**; NSA/CSS IG; [redacted]

~~(S)~~ **Background**. The OIG is completing a regional review of [redacted] that are focused on [redacted] including support to counterterrorism. Our review assesses site operations, compliance with intelligence oversight requirements, [redacted]

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) **Special Studies of Presidentially-authorized Program**; NSA/CSS IG

(U//~~FOUO~~) **Background**: The OIG is performing continual audits of NSA's Presidentially-authorized counterterrorism program. The overall objectives are to determine whether there are appropriate policies and procedures in place for activities under the program consistent with the terms of the Presidential Authorization; to evaluate their efficiency and effectiveness in mitigating any high-risk activities associated with the program; and to identify any impediments to satisfying the requirements of the Presidential Authorization.

(b) (3)-P.L. 86-36

(U) Planned

(U) **Followup Review of Access to SIGINT Databases**; NSA/CSS IG; ST-06-0003

(U//~~FOUO~~) **Backgound.** Information sharing and data access continue to be major priorities across the Intelligence Community (IC). To jumpstart the information-sharing concept, several efforts were initiated, most notably [redacted]

[redacted] counterterrorism activities. The objectives will be to determine if SID's process for granting database access is having the desired outcome, and, if not, what are the impediments. Additionally, we will determine the adequacy of security practices for terminating access once access is no longer needed.

(b)(3)-P.L. 86-36

(U) SEMIANNUAL REPORT TO THE CONGRESS

For the Period April 1, 2005 Through September 30, 2005

(U) **Kunia Regional Security Operations Center**; NSA/CSS IG; INSCOM IG; AIA IG; NSG IG; JT-05-0001; 31 March 2005

Summary. (U~~//FOUO~~) A team of inspectors from the Service Cryptologic Elements and NSA conducted a joint inspection of the Kunia Regional Security Operations Center (KRSOC). KRSOC is the first Regional Security Operations Center to be inspected by the Joint IG Team since the issuance of NSA/CSS Policy 1-3, *NSA/CSS Governance*, and the announcement of the NSA/CSS Build-Out. We found the site Headquarters relationship to be generally positive; some costly site-directed initiatives had not been coordinated with Higher Headquarters; and communication between KRSOC leadership and the SIGINT Analysis and Production Directorate needs attention, especially in light of the NSA/CSS Build-Out, which will require close collaboration in order to succeed.

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//MR

Category. (U) Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

(U) **Attack Sensing and Warning Program (Followup)**; NSA/CSS IG; ST-05-0014; 28 April 2005

Summary. (U~~//FOUO~~) The purpose of the Attack Sensing and Warning (AS&W) Program is to protect [redacted] The 2004 audit report found that the AS&W program had not undergone the type of independent review required by DoD and NSA regulations for high-dollar programs. As a result of our followup review, we were able to close out four of the six recommendations made in the 2004 final report. We found two recommendations that management had not addressed: The Defensive Information Operations Group has not developed the documentation required by DoD and NSA acquisition regulations and the same Group did not assign a qualified acquisition manager to the program as required by DoD and NSA acquisition regulations.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Infrastructure and Environment

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: ~~20291123~~

(U) **Cryptologic Mission Management Program**; NSA/CSS IG; AU-04-0005; 3 May 2005

Summary. (U//~~FOUO~~) We found the Cryptologic Mission Management (CMM) Program Management Office was staffed by qualified and experienced acquisition and engineering personnel focused on program results and compliance with DoD and Agency acquisition management requirements. However, a recent review by an Integrated Process Team (IPT), led by the Agency's Chief Systems Engineer, made recommendations to help reduce technical and other program risks. Carrying out the IPT recommendations will postpone the Milestone B decision for CMM Increment 1 from the end of September 2004 to May 2005. Specifically, our audit found problems with the CMM risk reduction efforts known as the Focused Demonstration Operational Capability in the following areas: Award Fee determination; Deliverables; and Unverified Costs.

Management Action. (U//~~FOUO~~) Management is acting on all but one of our recommendations. The SAE nonconcurred with our recommendation to establish a process to resolve major disagreements on the award fee. Our recommendation is necessary to prevent future arbitrary award fee decisions as well as fraud or wrongdoing. Therefore, we are requesting that SAE reconsider his nonconcurrence.

Overall Report Classification. (U) TOP SECRET//COMINT//MR

Category. (U) Acquisition Processes and Contract Management

(U//~~FOUO~~) **Nuclear Weapons Personnel Reliability Program**; NSA/CSS IG; AU-04-0010A; 26 May 2005

Summary. (U//~~FOUO~~) The purpose of the Nuclear Weapons Personnel Reliability Program (NWPRP) is to ensure that everyone who performs Nuclear Command and Control (NC2) duties meets the highest standards of reliability. Our audit found that the [redacted] strengthened the NWPRP control environment by implementing the recommendations from our 2002 review, but the following issues need attention: [redacted]

Management Action. (U//~~FOUO~~) Management agreed to implement a formal training program for NWPRP management and support personnel designate the Staff Security Officer as the official responsible for advising the program on security eligibility; establish formal procedures for NWPRP drug testing; and formally determine the status of [redacted]

Overall Report Classification. (U) CONFIDENTIAL//MR (b)(3)-P.L. 86-36

Category. (U) Joint Warfighting and Readiness

(U) **Office of Equal Employment Opportunity;** NSA/CSS IG; ST-05-0002; 1 June 2005

Summary. (U) The study found that mandated timelines related to the investigation of formal Equal Employment Opportunity (EEO) complaints are not being met. In addition, data related to EEO complaints, which must be posted on the Agency's public website, was incomplete and inaccurate, and NSA's FY2004 EEO Program Status Report, due by 31 January 2005, was not submitted to the Equal Employment Opportunity Commission until late April.

Management Action. (U) Management concurred with the recommendations to correct the issues described above.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Human Capital

(U) **Classified Material Destruction;** NSA/CSS IG; ST-05-0022; 7 June 2005

Summary. (U~~//FOUO)~~ An anonymous complaint sent to the Director, NSA and the Office of Inspector General (OIG) alleged that Eagle Alliance (EA) was utilizing government resources and processes to dispose of EA computer equipment. The GROUNDBREAKER contract stipulates that EA is responsible for disposal of EA computer equipment. The complaint also stated that EA did not have standard operating procedures (SOPs) for disposing of computer equipment. Our special study found no evidence that EA was using government resources to dispose of EA-owned computer equipment. However, EA has not instituted two elements required by the contract: written SOPs covering its disposal process and a process for disposing of hard drives after removal from EA-owned computers. We also found that EA is storing approximately [redacted] We recommended an immediate decision to either have the Agency take over the disposal function (amending the contract accordingly) or require EA to comply with the contract terms.

Management Action. (U) EA will provide its position in writing to the Maryland Procurement Office. Senior officials will then present the Agency's approach in writing to the OIG.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Acquisition Processes and Contract Management

(U) **Contract Rates for Office Space;** NSA/CSS IG; AU-04-0019; 8 June 2005

Summary. (U) NSA has operated under a model that collocates contractors with the

(b)(3)-P.L. 86-36

missions they serve. Our audit found that Contracting Officer's Representatives (CORs) were not validating on- and off-site costs charged for the contracts in our sample. Since overhead rates for work done at contractor facilities are usually higher than for government facilities, NSA could be paying off-site rates for contractors who are actually working on-site.

Management Action. (U) The Maryland Procurement Office agreed to issue guidance that requires contractors to provide a breakout of on- and off-site rates and hours on invoices and to require CORs to check the on- and off-site rates and hours.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Acquisition Processes and Contract Management (b)(3)-P.L. 86-36

(U//~~FOUO~~) **Followup Inspection: Special U.S. Liaison** NSA/CSS IG; INSCOM IG; NSG IG; AIA IG;

Summary. (U//~~FOUO~~) A followup joint inspection of the Special U.S. Liaison NSA/CSS found significant progress from the April 2004 joint IG inspection in the areas of training, intelligence oversight, security, communications, and information assurance. Civilian employee recruitment has improved, albeit slowly; however, several findings remain open, pending action by NSA Headquarters.

Management Action. (U) Management concurred with the recommendations and is taking appropriate corrective action.

Overall Report Classification. (U) SECRET//COMINT//REL TO USA, CAN, GBR, and NZL//20291123

Category. (U) Joint Warfighting and Readiness

(U) **Tailored Access Operations;** NSA/CSS IG; ST-04-022C; 19 July 2005

Summary. (U//~~FOUO~~) This study, the third in a series of three reports on the Agency's Tailored Access Operations (TAO) office, focused on the control environment. We found that: 1)

Management Action. (U) TAO management concurred with all OIG recommendations and plans to take corrective action by 1 October 2005. The Finance Directorate will move the reimbursement process to the Disbursing Office to

Overall Report Classification. (U) TOP SECRET//COMINT//NOFORN//220291123

Category. (U) Joint Warfighting and Readiness

(U) **FY2005 Report on Compliance With The Federal Information Security Management Act at NSA/CSS;** NSA/CSS IG; AU-05-0004; 5 August 2005

Summary. ~~(C)~~ NSA is making a concerted effort to address the weaknesses identified in our FY2004 audit of compliance with The Federal Information Security Management Act (FISMA). Although impediments still exist to achieving the Agency's certification and accreditation (C&A) goals, the Chief Information Officer (CIO) has made progress. NSA continued to maintain and track a Plan of Action and Milestone to address the inadequate C&A of Agency systems, identified as a material weakness in FY2002. However, we discovered several weaknesses in the Agency's IT security posture during our FY2005 FISMA review. We found that NSA has [redacted]

Management Action. (U~~//FOUO~~) The CIO has made a concerted effort to address FISMA requirements. This includes holding regular FISMA working group meetings, providing a data call to all responsible organizations to address reporting requirements, and raising awareness of FISMA requirements. In addition, the CIO established labs to perform vulnerability testing and penetration testing and secured additional resources to help create the documents associated with certifying mission-critical systems.

Overall Report Classification. (U) TOP SECRET//COMINT//NOFORN//20291123

(b) (3)-P.L. 86-36

Category. (U) Information Technology Management

(U) **NSA/CSS Representative Pacific (NCPAC);** NSA/CSS IG; IN-05-0002; 16 August 2005

Summary. (U~~//FOUO~~) Our inspection found that the Agency is well represented by the NSA/CSS Representative (NCR) Pacific and his staff. Pacific Command (PACOM) officials we interviewed had a high opinion of the NCR and his staff and regard them as a "model" of effective NSA/CSS liaison. Innovative NCPAC initiatives include embedding over [redacted] of the NCPAC staff in PACOM activities. Increased levels of support in the information operations arena are also highly valued by the Command. Areas for improvement include the following: NSA/CSS Policy 1-3 on governance does not conform to actual practice in the Pacific Theater; the operational span of control for the NCR is unclear; [redacted] the Regional Communications Security Monitoring Center, does not have enough assignees to perform its mission; and NCPAC's representational efforts to PACOM sub-commands in regard to Information Assurance are insufficient.

(b) (3)-P.L. 86-36

(b)(3)-P.L. 86-36

Management Action. (U) Management concurred in all recommendations, nine of which are already closed.

Overall Report Classification. (U) SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

Category. (U) Joint Warfighting and Readiness

(U) NSA/CSS IG;

Summary. (U~~//FOUO~~) Our inspection of the organization found that major development programs, including have potential, but their ultimate success at the Directorate and Agency levels. The Signals Intelligence Directorate leadership must act quickly to manage the risks

Management Action. (U) The Director for Analysis and Production concurred with all of the recommendations and convened an Integrated Product Team to address them.

Overall Report Classification. (U) SECRET//REL TO USA, AUS, CAN GBR, and NZL//20291123

Category. (U) Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

~~(S)~~ NSA/CSS IG

Summary. ~~(S)~~ We visited three sites selected on the basis of location, risk, and reported oversight issues. Based on our findings, a representative of SID is working with one of the sites to improve analysis and reporting on SIGINT collected there, while another site launched a comprehensive reassessment of its ability to contribute to the national SIGINT mission and satisfy the requirements of We also recommended that sites improve their emergency action procedures. To that end, has now clarified its emergency operations procedures, and agreed to conduct emergency drills.

Overall Report Classifications. (U) TOP SECRET//COMINT//20291123 (all three reports)

Category. (U) Joint Warfighting and Readiness

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(U) **Electronic Intelligence (ELINT) Modernization Program;** NSA/CSS IG; AU-05-0001; 19 September 2005

Summary. ~~(S)~~ Budgeted to receive [redacted] from FY2004-11, the ELINT Modernization Program is intended to develop, integrate, and deploy the capabilities needed to fill the gaps identified in a study conducted at the behest of Congress. The audit identified two significant problems: [redacted]

Management Action. (U) Management concurred with all recommendations and corrective action is underway.

Overall Report Classification. (U) SECRET//TALENT KEYHOLE//20291123

(b)(3)-P.L. 86-36

Category. (U) Joint Warfighting and Readiness

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) [redacted] NSA/CSS IG; INSCOM IG; AIA IG; NSG IG;

Summary. ~~(C)~~ A team of inspectors [redacted]

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

Category. (U) Joint Warfighting and Readiness

(U) **Precious Metals Recovery Program;** NSA/CSS IG; ST-05-0005; 19 September 2005.

Summary. (U~~//FOUO~~) The Precious Metals Recovery Program (PMRP) recycles film, circuit boards, and microchips for NSA, DoD, and other Intelligence Community customers. Our special study found that the PMRP [redacted] and no formal plan to spend the funds [redacted] generated from recycling microchips.

(b) (1)
(b) (3)-P.L. 86-36

Additionally, the policy establishing the PMRP has not been updated since 1991, and internal controls are needed to safeguard the precious metals that are recovered when microchips are recycled.

Management Action. (U~~//FOUO~~) Management nonconcurred with our recommendation to develop a plan to spend these funds rather than letting the money accumulate. Consequently, we are forwarding the report to the Comptroller.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Other

(U) [redacted] NSA/CSS IG; [redacted]

Summary. ~~(S)~~ Our functional inspection of NSA's program to [redacted] which is managed by the Signals Intelligence Directorate (SID), focused on analysis and training with the goal of determining whether SIGINT analysts [redacted] We found that Agency and SID leaders have not conducted a risk assessment to determine the appropriate level of effort for [redacted] and Agency policy does not adequately address the authorities and responsibilities for this function. Moreover, NSA's Implementation Plan for [redacted] does not address a key goal of the Director of Central Intelligence: [redacted]

Management Action. (U) Management concurred with our recommendations and is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//REL TO USA, AUS, CAN, GBR, NZL//20291123

Category. (U) Joint Warfighting and Readiness

(b) (3)-P.L. 86-36

(U) **Information Technology Directorate Field Liaison Division;** NSA/CSS IG; IN-05-0005; 20 September 2005

Summary. (U~~//FOUO~~) The Information Technology Directorate's (ITD) Field Liaison Division is a [redacted] organization created in January 2003 as a direct response to recommendations from several Joint IG inspections. During the inspection, the Field Liaison Division's leadership changed and the ITD restructure began, resulting in a new focus for the Division. Nevertheless, the Director for IT asked that we proceed with the inspection to help identify problems or issues that need to be considered in ITD's restructuring and consolidation efforts. To this end, we issued a letter report advising the Director for IT of areas in need of attention as the ITD consolidation continues. Our inspection found that the Field Liaison Division has had a positive effect on the Extended

Enterprise; however, as ITD implements its concept of centralized management with decentralized execution, close attention should be given to the following: clearly delineating roles and responsibilities; implementing a mechanism for assessing the effectiveness of the new structure; and providing a dynamic, up-to-date, and useful NSANet presence.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Information Technology Management

(U) **Meade Operations Center;** NSA/CSS IG; INSCOM IG; AIA IG; NSG IG; JT-05-0006; 30 September 2005 (b)(3)-P.L. 86-36

Summary. (U//~~FOUO~~) The Joint IGs conducted an inspection of the [redacted] Meade Operations Center (MOC)) in 2002. A followup inspection in 2003 assessed progress in several areas, including Command Topics and Mission Operations. In keeping with the three-year inspection cycle for major field sites, the Joint IGs scheduled an inspection of the MOC to begin in August 2005. Our preparation for this inspection revealed that the predominant theme of the two previous inspections remains unresolved – the persistent lack of documented mission and an effective governance mechanism or chain-of-command. In a Joint IG Management Advisory Report, the Joint IGs suspended the on-site phase of the inspection until the Signals Intelligence Directorate (SID) clearly documents a mission and begins to exercise an effective governance approach for the organization. The Joint IGs concluded that the unresolved issues are unlikely to improve without a zero-based review to determine the missions, if any, that are best performed by the MOC, and 2) the implementation of effective governance from SID of those missions.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Joint Warfighting and Readiness

(U) **Inappropriate Representation Before the Government and Misuse of Resources;** NSA/CSS IG; IV-05-0005; September 2005

Summary. (U//~~FOUO~~) An NSA/CSS employee who established a software company inappropriately represented his company in a "pitch" meeting before the Government. This employee also misused Government resources to solicit and conduct private business. Furthermore, the employee and his business associate knowingly misused Government Information Systems to solicit business for their private company. Due to the potential Title 18 violation, the matter was referred to the DoJ for a prosecutive opinion.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Personnel/Standards of Conduct; Procurement and Contract Administration

(U) **Inappropriate Representation Before the Government;** NSA/CSS IG; IV-05-0011; June 2005

Summary. (U~~//FOUO~~) An NSA employee who "moonlighted" part-time for an Agency contractor inappropriately represented the contractor in a meeting before the Government, in a particular matter in which the United States was a party and had a direct interest. Due to the potential Title 18 violation, our report was referred to the DoJ for a prosecutive opinion.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Personnel/Standards of Conduct

(U) **Time and Attendance Investigations**; NSA/CSS IG; IV-04-0040 (31 May 2005); IV-05-0008 (23 May 2005); IV-05-0023 (9 September 2005); IV-05-0032 (9 September 2005)

Summary. (U~~//FOUO~~) The OIG substantiated four allegations of Time and Attendance abuse, wherein employees claimed hours in excess of those they were determined to have actually worked. In the aggregate, these cases will result in the recovery of approximately $46,500.00 in funds paid to employees for hours falsely claimed.

Overall Report Classifications. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

Category. (U) Other (Fraud)

(U) SEMIANNUAL REPORT TO THE CONGRESS

For the Period October 1, 2004 Through March 31, 2005

(U~~//FOUO~~) **Timecard Accountability in Tailored Access Operations**; NSA/CSS IG; ST-04-0022A; 20 October 2004

Summary. (U~~//FOUO~~) This special study investigated an anonymous Hotline complaint regarding two timesheet issues that warranted immediate attention by Tailored Access Operations (TAO) management. We found that TAO's [redacted] lacked controls to ensure that hours entered into the payroll system matched the hours certified by supervisors. We also noted inconsistent application of pay entitlements for Access Operations personnel who improperly claimed regular duty time as well as overtime and/or compensatory time for time spent traveling outside their normal work schedule.

Management Action. (U) TAO agreed to publish timekeeper verification procedures and to obtain an opinion from Human Resources/Compensation Policy on travel time compensation, premium pay entitlements, and scheduling duty hours for personnel required to travel for TAO mission exigencies. TAO also assured the NSA/CSS Office of the Inspector General that this opinion would be applied consistently across the organization.

Overall Report Classification. (U) CONFIDENTIAL//X1

Category. (U) Human Capital

(b)(3)-P.L. 86-36

(U) **Yakima Research Station;** NSA/CSS IG; NSG IG; JT-04-0014; 3 December 2004

Summary. ~~(C)~~ A joint team of inspectors from the Naval Security Group and NSA conducted a joint inspection of the Yakima Research Station (YRS). Our findings focused on the lack of compliance with regulations and policies. We also noted the lack of guidance and support from NSA Headquarters (HQ), especially involving mission focus and resources. As to mission focus, we found that YRS is strategically adrift and requires a mission review; NSA needs to validate the site's mission and make better use of its talented workforce. Regarding resources, dramatic changes in the site's technical and analytic resources in recent years were not accompanied by a cost-benefit analysis of the requirements.

Management Action. (U) Management at YRS and HQ are taking corrective action on all of the findings.

Overall Report Classification. (U) TOP SECRET//COMINT/REL TO USA, AUS, CAN, GBR, and NZL//X1

Category. (U) Joint Warfighting and Readiness

Derived From: NSA/CSSM 123-2
Dated: 24 February 1998
Declassify On: Source Marked ~~X1~~

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(U) **Contractor Space**; NSA/CSS IG; AU-04-0001; 13 January 2005

Summary. (U~~//FOUO~~) The lack of space has reached crisis proportions at NSA. The current occupancy rate of 97.4 percent is projected to reach 101.4 percent by the end of FY2005. A major factor is the need to house contractors, who now exceed the civilian workforce. Our audit found that current policy and planning vehicles are incapable of producing the long-term comprehensive plan needed to manage the crisis and to track the contractor presence at NSA. We also found that recent initiatives by the Associate Director of Installations and Logistics (ADIL) and the Senior Acquisition Executive (SAE) to relieve the Agency's space shortage by removing contractors were lacking key elements such as: 1) a formal policy and process for producing a comprehensive long-term facilities plan aligned with the NSA/CSS strategic plan; 2) short-term plans to relocate people on existing contracts do not specify how removal costs (estimated at over [redacted] from FY2005-08) will be funded, nor do they give criteria for selecting which contractors to move; and 3) NSA needs an explicit, enforceable policy on allowing contractors to work in Agency spaces.

Management Action. (U~~//FOUO~~) The ADIL and SAE nonconcurred on the grounds that some actions were already in progress before the audit. Our report recognizes these initiatives, but they are not completed. Moreover, ADIL and SAE have not agreed to set criteria for deciding which contractors on existing contracts to remove; in the opinion of General Counsel, this leaves the Agency vulnerable to charges of favoritism. Consequently, we referred this report to DIRNSA and he directed ADIL and SAE to take management action.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Infrastructure and Environment

(b) (3)-P.L. 86-36

(U~~//FOUO~~) [redacted] NSA/CSS IG; [redacted]

Summary. ~~(S)~~ Our inspection of the [redacted] found some duplication of effort resulting from mission overlap within [redacted] itself and with other organizations in the Analysis and Production Directorate (SID/S2). We found that: [redacted] and across S2 leads to duplication of effort [redacted] it is critical to formalize all aspects of information sharing in Memorandums of Understanding with parent agencies that have integrees in [redacted] relationships with [redacted] elements need attention - customers need to know exactly what to provide in a Request for Information and to be kept apprised of the status of their requests; and leadership at the S2, SID, and Agency levels is not adequately engaged in the [redacted] support mission which has created an adverse effect on [redacted] morale and staffing.

Management Action. (U) Issues related to information sharing and customer relationships are now being addressed. [redacted] new management is planning an aggressive approach to tackle these issues and to improve [redacted]

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//MR

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

Category: (U) Joint Warfighting and Readiness

~~(C)~~ **Special Study of Tailored Access Operations**; NSA/CSS IG; ST-04-0022B; 15 February 2005

Summary. ~~(S)~~ A special study found that the [redacted] 2005 program has experienced schedule slippage that [redacted] In addition, cost overruns on the [redacted] 2005 procurement may exceed [redacted] Poor communication and coordination within the Tailored Access Operations (TAO) organization, which manages [redacted] and related efforts, have impeded the success of the [redacted] initiative. Specifically, the special study found that: 1) the [redacted] Program Manager (PM) lacked the authority needed for effective oversight of the [redacted] 2005 program; 2) the [redacted] 2005 PM did not effectively engage other TAO Offices, especially the [redacted] Program Management Office, in defining [redacted] 2005 requirements; and 3) Program progress was not always accurately assessed and reported to Agency leaders.

Management Action. (U) The TAO Group Chief has assumed the role of [redacted] PM and realigned the [redacted] PM organization directly under her. She plans to formalize the [redacted] Team structure to enhance communication, clearly define requirements, and foster teamwork within TAO and with the contractor.

Overall Report Classification. (U) TOP SECRET//COMINT//ORCON, NOFORN//MR

Category. (U) Acquisition Processes and Contract Management

(U) [redacted]
NSA/CSS IG; [redacted]

Summary. ~~(S)~~ A Joint Inspectors General team concluded that implementation of the [redacted] while progressing, got off to a poor start and is currently impeded by leadership disagreements and procedural differences between the parent Agencies. The Directors of the Agencies must ensure that senior leaders at [redacted] are fully committed to implementing the [redacted] Specific findings of this joint review include the following: 1) the four missions that have already transitioned to the [redacted] are beginning to produce the desired synergies; 2) while the four implementing documents of spring 2004 suffice in the short term, they do not provide sufficiently detailed, long-term direction needed to fully implement the [redacted] concept and ensure productive and efficient operations; 3) senior leaders have not resolved the leadership disagreements at the site, which stem from widely diverging views on [redacted] implementation; and 4) officials need to resolve implementation and procedural differences regarding foreign partner information sharing, funding, and the management of human resources.

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

Management Action. (U) Management concurred with the recommendations directed to their respective offices. A number of efforts are underway to implement the recommendations, and several actions have been completed.

Overall Report Classification. (U) SECRET//COMINT//TALENT KEYHOLE//NOFORN//25X1

Category. (U) Joint Warfighting and Readiness

(b) (1)
(b) (3)-P.L. 86-36

~~(C)~~ NSA/CSS IG; INSCOM IG;

Summary. ~~(S)~~ A Joint Inspectors General team from INSCOM and NSA/CSS conducted an inspection at The team found problems that have a direct impact on the site's effectiveness. The most significant issues facing the site's The report has been provided for information purposes to appropriate NSA elements. The NSA/CSS OIG will follow up on many of the issues in the report during our 2005 joint IG inspection of

Management Action. (U) Management concurred with the recommendations and is taking appropriate corrective action.

Overall Report Classification. (U) SECRET//COMINT//MR

Category. (U) Joint Warfighting and Readiness

(U) **Possible Violation of Federal Law;** NSA/CSS IG; IV-04-0047; 28 October 2004

Summary. (U~~//FOUO~~) Pursuant to a 1995 agreement between the Department of Justice (DOJ) and the agencies of the Intelligence Community, the NSA/CSS General Counsel referred allegations of possible criminal conduct by an NSA employee to the DOJ. The results of the OIG inquiry into this matter were also forwarded to DOJ.

Overall Report Classification. (U) TOP SECRET//COMINT//X1

Category. (U) Other (Intelligence Oversight)

(U) **Time and Attendance Investigations**; NSA/CSS IG; IV-04-0056 (16 November 2004); IV-04-0064 (5 November 2004); IV-05-0001 (22 December 2004)

Summary. (U~~//FOUO)~~ The OIG substantiated three Time and Attendance abuse allegations, wherein employees claimed hours in excess of those they were determined to have actually worked. In the aggregate, these cases will result in the recoupment of almost $20,000.00 in funds paid to employees for hours falsely claimed. Two of these cases were referred to the DOJ for possible prosecution for violation of 18 U.S.C. § 287 and 18 U.S.C. § 1001.

Overall Report Classifications. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY (all referenced investigations)

Category. (U) Other (Fraud)

(U) **Misuse of Resources;** NSA/CSS IG; IV-04-0054; 8 February 2005

Summary. (U) The OIG substantiated an allegation that an Agency employee was using Agency computer systems to manufacture counterfeit rebate coupons for submission to commercial computer manufacturers for personal gain. Disciplinary action is pending, and the case was forwarded to the NSA/CSS Office of General Counsel for referral to the DOJ.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Other (Misuse of Resources)

(U) SEMIANNUAL REPORT TO THE CONGRESS

For the Period October 1, 2003 Through March 31, 2004

(b) (3)-P.L. 86-36

(U) **Meade Operations Center-Followup Inspection**; NSA/CSS IG; INSCOM IG, AIA IG, NSG IG, JT-03-0005, 3 October 2003

Summary. (U//~~FOUO~~) The followup inspection found that the [redacted] the Meade Operations Center, [redacted] but was still awaiting a decision on its governance and its place in the organizational structure. Morale had improved under new, stable leadership. We recommended that the Signals Intelligence Directorate (SID) assign a suspense date to finalize its proposal for governance and to place an agenda item titled "Implementation Plan for MOC Governance" at the next Joint Issues Board Meeting.

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//X1

(b) (1)
(b) (3)-P.L. 86-36

Category. (U) Joint Warfighting and Readiness

~~(S)~~ [redacted] NSA/CSS IG, [redacted]

Summary. ~~(S)~~ We visited selected [redacted] sites to ensure that policies and internal controls for its intelligence activities are carried out with due regard for the law. We found that processes exist to validate that intelligence activities comply with the law; however, we also found four areas of concern regarding policies and internal controls: [redacted]

Management Action. (U//~~FOUO~~) Management concurred with all recommendations and agreed to publish formal policies and agreements that reflect current responsibilities; incorporate OIG suggestions to improve the control environment; conduct rigorous security reviews—and act on the results; and ensure that valuable SIGINT assets are both properly safeguarded and fully utilized.

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//X1

Category. (U) Joint Warfighting and Readiness

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: ~~X1~~

(U~~//FOUO~~) **Deployment Services, Analysis and Production Directorate**; NSA/CSS IG, IN-03-0003, 21 November 2003

Summary. (U~~//FOUO~~) The Deployment Services organization in the Analysis & Production Directorate (A&P) was created to optimize agility in responding to rapidly changing intelligence needs. The organization also manages the training and development of the analytic work force. We found that Deployment Services did a good job of getting the right person in the right job at the right time—particularly in a crisis—and had forged effective partnerships with the Associate Directorates of Human Resource Services (ADHRS) and Education and Training (ADET). However, workforce development needed attention from A&P leadership, starting with an analysis of future training needs engendered by new toolsets. Human resource databases, developed and maintained by Deployment Services staff, are labor intensive. PeopleSoft database services from ADHRS should eventually allow production personnel to concentrate on mission-centric work.

Management Action. (U) A&P Directorate, Deployment Services, ADHRS, and ADET are taking corrective action on all of the recommendations.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Human Capital

(b)(3)-P.L. 86-36

(U) **Information Assurance Solutions Division**; NSA/CSS IG, IN-03-0009, 23 December 2003

Summary. (U~~//FOUO~~) The Information Assurance Directorate's (IAD) [redacted] The division follows a well-documented process and methodology, and earns high praise from its customers regarding risk management. The inspection found that the division was accepting many projects that did not meet [redacted] requirements; in order to perform testing, the [redacted] division had to do the customer's work—a waste of Agency resources. Long lulls between projects were inefficient and frustrating to the division's cadre of technical experts. Correcting the problem depends on an effective IAD-wide requirements and prioritization process and a mechanism to deploy [redacted] skills where they are most needed.

Management Action. (U~~//FOUO~~) The [redacted] division has since been reassigned to the [redacted] as part of the IAD reorganization. This reassignment of the [redacted] function should resolve most of the concerns specific to the [redacted] division. The larger IAD issues are addressed in our special study on IAD Corporate Issues.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Information Technology Management (Systems Security)

(U) **Ft. Gordon Regional Security Operations Center**; NSA/CSS IG, INSCOM IG, AIA IG, NSG IG, JT-04-0001, 13 January 2004

Summary. ~~(C)~~ A joint inspection of the Ft. Gordon Regional Security Operations Center (GRSOC) by a team from the Service Cryptologic Elements and NSA/CSS found problems that directly affected the site's effectiveness and must be addressed at a high level: (1) assigning enough people and resources to accomplish the expanding mission; (2) acquiring space to accommodate mission growth and a continuity of operations facility; and (3) specifying which Headquarters organization is responsible for resolving field mission and support problems. The team also found two perennial problems that are not confined to GRSOC and require innovative solutions by senior leadership: (1) [redacted] (2) "Jointness Initiatives" are not getting the level of Higher Headquarters support needed for success.

Management Action. (U) Management is taking appropriate corrective action.

Overall Report Classification. (U) TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//X1

(b)(3)-P.L. 86-36

Category. (U) Joint Warfighting and Readiness

(U) **Vulnerability Assessments Division**; NSA/CSS IG, IN-03-0004, 23 January 2004

Summary. ~~(C)~~ Vulnerability assessments are an important tool to help protect the nation's critical infrastructure of telecommunications and information systems, per National Security Directive 42 (NSD-42) and Presidential Decision Directive 63. The Vulnerability Assessment division is part of the Discover Vulnerabilities (DV) triad of services offered by IAD organizations; it performs high-level assessments that identify vulnerabilities in the operational information systems of DoD, Intelligence Community, and selected private sector customers. The inspection found that the organization provides a valuable service and enjoys a high degree of customer satisfaction, but the workload, at the time of the inspection, was uneven and insufficient for the [redacted] assignees. Moreover, information sharing with other Triad members and with the larger DV community is minimal. Two issues that contribute to the division's workload problems are the absence of both a centrally managed IAD requirements process and a single codified management process for the triad of DV services.

Management Action. (U) Management has already taken steps to improve its control environment, particularly in the area of time and attendance. Recommendations that require action above the Vulnerability Assessment division, symptomatic of larger IAD process and policy issues, are addressed in our special study on IAD Corporate Issues.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Information Technology Management (Systems Security)

(U) **Selected System Engineering Contracts**; NSA/CSS IG, ST-03-0019, 30 January 2004

Summary. (U//~~FOUO~~) This special study reviewed [ ] system engineering contracts to ensure proper competition. We found that only [ ] were sole source actions, and they were supported by Competition in Contracting Act (CICA) justifications and documentation. The remaining actions were either 8(a) awards to small disadvantaged businesses, orders legitimately placed on previously awarded competitive actions, or competitively awarded contracts. We did identify potential issues with [ ] sole source contracts regarding questionable cost growth, continuing lack of competition, and failure to perform market research. These [ ] contracts will be covered in a separate report.

Management Action. (U) The Acquisition organization and the Competition Advocate recently took steps to make it more likely that competition would be utilized to the maximum extent practicable.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Acquisition Management

(b)(3)-P.L. 86-36

(U) **Information Assurance Directorate – Corporate Issues**; NSA/CSS IG, ST-03-0016, 19 February 2004

Summary. (U//~~FOUO~~) Organizational inspections of three IAD divisions, two of which are summarized in this Semiannual Report (Information Assurance Solutions and Vulnerability Assessments) and one from the previous Report (Operational Network Evaluations) surfaced four common themes regarding IAD corporate functions that negatively impact the overall Discover Vulnerabilities (DV) activity. This study offered an overarching view of how DV processes are sometimes at cross-purposes with one another and recommended measures to align them with corporate IAD goals. Key findings of the study that warrant further corporate attention are: (1) a porous IAD requirements process that is not centralized and lacks sufficient corporate structure and oversight to ensure consistent handling of customer requests; (2) an ineffective, non-cohesive corporate marketing strategy; (3) lack of central management of DV activities; and (4) ineffective knowledge management.

Management Action. (U) IAD leadership concurred with all of the recommendations and has begun to implement corrective measures to address the findings.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Information Technology Management

(U) **Summary of OIG Efforts Related to the Congressional Joint Inquiry Into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001**; NSA/CSS IG, ST-04-0015, 25 February 2004

Summary. (U//~~FOUO~~) The IG, DoD has started a review of the Factual Findings and Record of the "Joint Inquiry Into Intelligence Community Activities Before and After

the Terrorist Attacks of September 11, 2001," dated 10 December 2002. Specifically, Recommendation 16 of this report tasks the IG, DoD to review the findings and record of the Joint Inquiry "to determine whether and to what extent personnel at all levels should be held accountable for any omission, commission, or failure to meet professional standards." On 12 November 2003, the Director, NSA wrote to the Congress in response to Recommendation 10 of the same report. His letter referred to a series of specific areas in which the Agency has been energetically responding to the issues that gave rise to the recommendation.

(U) At the request of the DoD Deputy Inspector General for Intelligence, the NSA OIG summarized its efforts related to the Director's response. Since 2001, about half of the OIG's reviews, including inspections, audits, and special studies, have been germane to the Director's response. The NSA OIG's report summarized 55 reviews (over 40 completed) for the period 2001 to 2004. The OIG grouped the reviews into two categories: *technological solutions and programs* (includes research and technology initiatives, acquisition management, organizational transformation, and mission and systems security); and *collaboration and information sharing* (includes relations with partners and customers, and joint inspections with the service cryptologic elements). It should be noted that the summary of each review describes conditions as they existed at the time of the review. Those conditions may be, and in many cases certainly are, materially different as of the date of this Semiannual Report.

Overall Report Classification. (U) TOP SECRET//COMINT/TALENT KEYHOLE//REL TO USA, AUS, CAN, GBR, and NZL//X1

Category. (U) Other

(b) (1)
(b) (3)-P.L. 86-36

(U) **Campaign Supplemental Funding**; NSA/CSS IG, AU-03-0004, 9 March 2004

Summary. ~~(S)~~ This report summarized the results of our audit of the supplemental funds NSA received to respond to the events of 9/11 and the invasion of Iraq. After 9/11, Congress bolstered the Agency's budget with four emergency supplemental appropriations [redacted] for the war on terrorism and the Iraqi conflict. NSA's Directorate of Finance (DF) had to manage these large supplemental appropriations under extraordinary pressure and time constraints. Our review focused on the first two supplemental appropriations, which were received from September 2001 to September 2002 and totaled [redacted] The audit found that when NSA requested the initial emergency supplemental, there was no formal process for developing and documenting this type of request and tracking the underlying requirements. Two factors made the task even harder: the Agency had only a short time in which to submit the requests, and DoD failed to issue specific guidance to supplement the general guidance published by OMB shortly after 9/11. The Agency's situation was not unique; as reported by GAO, DoD's failure to issue specific internal guidance caused uncertainty on appropriate uses of the emergency funds throughout its components. For the second supplemental, we encountered difficulty in completely tracking the actual expenditure categories in the accounting system to the requirement areas because the reporting "categories" did not correlate.

Management Action. (U~~//FOUO~~) Since the current administration plans to continue funding the war on terrorism through supplemental appropriations, it is important to have an efficient process for managing them; it should facilitate accurate accounting that tracks how funds are used to the approved requirement. DF recently developed a template (including description, justification, requested funds, initiating organization, and point of contact for documenting each requirement in a supplemental request) to standardize Agency requests for supplemental appropriations. Properly used, the template should ensure that requirements are documented and trackable, which will help maintain the Agency's credibility with Congress.

(b)(3)-P.L. 86-36

Overall Report Classification. (U) SECRET//X1

Category. (U) Financial Management

(U) **Report of Inquiry: Usefulness of** [redacted] **Analysis**; NSA/CSS IG, [redacted]

Summary. ~~(S)~~ In August 2003, an analyst alleged that he published a report in [redacted] and that the report's editing resulted in the deletion of a significant amount of information. The analyst believed that the deleted information would have been useful to other analysts [redacted] Our inquiry concluded that the editing was performed in accordance with established policies and procedures regarding sanitization of reports containing sensitive information. Additionally, the deleted information was retained for potential future use.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Overall Report Classification. (U) TOP SECRET//COMINT//X1

Category. (U) Other

(U) **Access to Signals Intelligence Databases**; NSA/CSS IG, IN-04-0001, 11 March 2004

Summary. (U~~//FOUO~~) A key NSA goal is to share information in Agency databases more freely among all parts of the extended enterprise and with Agency customers. Just as this inspection commenced, the Signals Intelligence Directorate (SID) announced a new policy for gaining access to these databases. As a result, we curtailed the inspection but made recommendations to ensure that access requests are handled in accordance with the new transformation goal. We found that SID's efforts to streamline database access had gathered considerable momentum.

Management Action. (U~~//FOUO~~) To sustain this momentum, SID officials agreed to publish a policy framework to guide those who make mission-related decisions on whether to grant access to SID databases; document the main steps in the new process, along with time limits for each step; and spell out the authorities, roles, and responsibilities of all parties involved in processing requests to access SID databases.

Overall Report Classification. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY

Category. (U) Joint Warfighting and Readiness

(U) **Possible Violations of Federal Law,** NSA/CSS IG, IV-04-0003, 12 March 2004

Summary. (U~~//FOUO~~) Pursuant to a 1995 agreement between the Justice Department and the agencies of the Intelligence Community, we requested that the NSA General Counsel refer to the General Counsel of another Intelligence Community agency allegations of possible criminal misconduct by an employee of that agency and the results of our inquiry.

Overall Report Classification. (U) TOP SECRET//COMINT//NOFORN//X1

Category. (U) Other

(U) **Time and Attendance Investigations**, IV-03-0022 (12 December 2003), IV-03-0047 (9 December 2003), IV-03-0059 (5 February 2004)

Summary. (U~~//FOUO~~) The OIG substantiated three separate and substantial "Time and Attendance Abuse" allegations where employees claimed hours in excess of what they actually worked. Combined, these cases will result in the recoupment of almost $30,000 in funds paid to employees for hours falsely claimed. One of these investigations uncovered rampant timecard abuse in one particular Agency organization and resulted in findings against six of that organization's employees.

Overall Report Classifications. (U) UNCLASSIFIED//FOR OFFICIAL USE ONLY (all three investigations)

Category. (U) Other

(b)(3)-P.L. 86-36

(U) **Attack Sensing and Warning Program**; NSA/CSS IG, AU-03-0003, 24 March 2004

Summary. ~~(S)~~ The purpose of the Attack Sensing & Warning (AS&W) program is to detect unauthorized intrusions or malicious attacks on DoD systems and networks. The audit looked at the Agency's [redacted] major AS&W projects. We found that this [redacted] program has never undergone the type of independent formal review required by DoD and NSA acquisition regulations. Furthermore, no one has determined when future program capabilities will be fielded and how much they will cost. The audit also found that the Defensive Information Operations officials have no formal process for passing research and development (R&D) topics or requirements to the Defense Computing Research Office.

Management Action. (U~~//FOUO~~) Management has agreed to place the AS&W program in the appropriate category, schedule a milestone review, conduct Operational Testing & Evaluation, and coordinate R&D efforts with the Defense Computing Research Office to share information and avoid duplication of effort.

Overall Report Classification. (U) SECRET//NOFORN//X1

Category. (U) Other (Major Acquisition Program)

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) **Counter Encryption Programs**; NSA/CSS IG, AU-03-0002, 31 March 2004

Summary. ~~(S)~~ The purpose of the audit was to determine if a counter encryption program is capable of meeting current and projected customer requirements to counter specific instances of strong encryption.

Management Action. (U) Management concurred in the recommendation to complete the necessary program documentation and to provide it to the MDA at the scheduled interim review date of April 2004.

Overall Report Classification. (U) TOP SECRET//COMINT-ECI-KES//X1

Category. (U) Other (Major Acquisition Program)

~~TOP SECRET//SI//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U) SEMI-ANNUAL REPORT TO CONGRESS
1 April to 30 September 2011

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~*20320108*~~

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide Intelligence Oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence Oversight is designed to ensure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The Intelligence Oversight mission is grounded in Executive Order 12333, which establishes broad principles under which Intelligence Community components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

(U) A MESSAGE FROM THE INSPECTOR GENERAL

(U) This report summarizes the more significant activities of the Office of the Inspector General (OIG) of the National Security Agency between 1 April and 30 September 2011. The report is mandated by the Intelligence Authorization Act of 2010.

(U) During the reporting period, the NSA OIG completed 59 audits, inspections, special studies, and investigations.

(U) The Audits Division completed five audits ranging from Information Technology to federal compliance to operations.

(U) The Inspections Division completed reports on two joint inspections of NSA field sites and one expeditionary operations review of [redacted] (b)(3)-P.L. 86-36

(U) The OIG completed five special studies of operations and intelligence oversight.

(U) The Investigations Division fielded 571 contacts from the OIG Hotline. The team opened 53 investigations and closed 46 in the reporting period.

(U) The office also completed internal quality assurance reviews of the Joint Inspection program and the follow-up process.

(U) Each report and special study contained recommendations on which the OIG and NSA management concurred, recommendations designed to improve the efficiency and effectiveness of the programs under review. The OIG tracks recommendations until they have been implemented and regularly reports to the NSA Director on the status of open recommendations. Of the 213 recommendations issued in the reporting period, 36 have been closed.

George Ellard

George Ellard
Inspector General

(U//~~FOUO~~) DISTRIBUTION:

DIR
ExDIR
CoS
SID Dir
IAD Dir
TD Dir
LAO
OGC
ODOC
FAD
BMI
SAE
ODNI IG
DoD IG

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(U) SIGNIFICANT PROBLEMS, ABUSES, AND DEFICIENCIES

(b)(3)-P.L. 86-36

(U//~~FOUO~~) OIG work during the reporting period did not reveal any particularly serious or flagrant problems, abuses, or deficiencies related to the administration of Agency programs and operations requiring immediate reporting to the Director and to Congress.

(U//~~FOUO~~) Completed reports did identify [ ] significant problems related to Agency operations and made appropriate recommendations. Agency managers agreed with all recommendations; however, corrective action plans were not provided for one of the [ ] significant recommendations.

(U) **Audit of Agency Controls for [ ] IT Hardware Purchases** (29 April 2011)

(U//~~FOUO~~) The audit concluded that the Agency's Supply Chain Risk Management (SCRM) strategy [ ]

(U) The audit included three significant recommendations: [ ]

(U) **Audit of Nuclear Command and Control (NC2)** (23 September 2011)

(U//~~FOUO~~) The NC2 program [ ] Since 2003, approximately [ ] recommendations related to NC2 have been made by auditors and vulnerability assessment teams. The focus of the current audit was to ensure that actions taken satisfied previous recommendations. In addition, the audit reviewed new problems discovered since the 2006 OIG audit.

(~~TS//NF~~) The audit revealed that all but [ ] recommendations have been adequately closed. Key recommendations from 2005 dealing with [ ] Appropriate corrective action has been taken for [ ]

(U) The audit made two significant recommendations:

- (U//~~FOUO~~) Complete the testing and approval requirements for the accountability system to provide 100 percent assurance of the [ ]
- (~~S//NF~~) [ ] and establish a timeline for completion. (Management did not provide a corrective action plan for this recommendation.)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Special Study of Non-Traditional Dissemination Methods: Dissemination Strategy Evaluation** (28 September 2011)

(U//~~FOUO~~) Since 2011, NSA has worked to address the challenges and opportunities presented by a Presidential call for increased information sharing. Various non-traditional dissemination methods have been implemented to facilitate that effort. The review, which focused on select processes and tools that analysts use for non-traditional dissemination, revealed that the Signals Intelligence Directorate (SID) does not have a comprehensive dissemination plan and that the Directorate's implementation of the IC-wide information-sharing system known as [redacted] resulted in confusion and overly restrictive limitations on its use.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) The report made three significant recommendations:

- (U//~~FOUO~~) Conduct a strategic review of dissemination policy and create a comprehensive dissemination plan.
- (U//~~FOUO~~) Re-evaluate the internal controls used for [redacted] and the operating principles for NSA/CSS participation in the tool.
- (U//~~FOUO~~) Update the [redacted] and announce the new guide to the analytic workforce.

(U//~~FOUO~~) SID took immediate steps to implement the two recommendations related to [redacted] and they have been closed.

(U) AUDITS

(b)(3)-P.L. 86-36

(U) Audits Completed in the Reporting Period

(U) **Agency Controls for** [redacted] **IT Hardware Purchases** (29 April 2011)

(U//~~FOUO~~) Because of the growing reliance on globally sourced Information Technology (IT), Agency systems and networks [redacted]

(U) **NSA Police (NSAP) Operations** (9 May 2011)

(U//~~FOUO~~) Controls over NSAP equipment inventories must be tightened, and NSA needs a formal agreement with Fort Meade for Vehicle Cargo Inspection Facility (VCIF) services. NSAP management lacks a process to determine needs for operational equipment and supplies. As a result, Agency funds are not used economically and efficiently and inventory records are inaccurate. [redacted] The Agency spends more than [redacted] a year in salary expenditures [redacted] K-9 teams) for approximately [redacted] NSA and Fort Meade vehicle and cargo inspections. The Agency must formalize the VCIF operation agreement with Fort Meade to ensure a clear understanding of roles and responsibilities. We referred this matter to the Office of General Counsel for review.

(U) **NSA/CSS Compliance with the Federal Information Security Management Act (FISMA)** (13 September 2011)

(U//~~FOUO~~) FISMA requires measurements of the adequacy and effectiveness of the federal government's information security environment and systems that operate within that environment. The audit details the Agency's efforts during the past year to improve IT processes and track Agency and system weaknesses. More work must be done [redacted]

(U) **Nuclear Command and Control (NC2)** (23 September 2011)

(U//~~FOUO~~) The NC2 program [redacted] Since 2003, approximately [redacted] recommendations related to NC2 have been made. We concentrated on [redacted] previous recommendations that we determined to be the most relevant. The focus of the current audit was to ensure that actions taken satisfied previous recommendations. In addition, the audit reviewed new problems discovered since a 2006 OIG audit.

(~~TS//NF~~) The audit revealed that all but [redacted] recommendations have been adequately closed. Key recommendations from 2005 dealing with [redacted] Management concurred with all [redacted] recommendations but did not provide corrective action plans for [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(U) Significant Recommendations Outstanding from Previous Semi-Annual Reports

(U) **Audit of Cross Domain Solutions (CDSs)** (23 June 2010)

(U//~~FOUO~~) The audit objective was to determine whether CDSs effectively and efficiently protect Agency networks. A CDS is a controlled interface that allows the secure transfer of data between domains with different security levels (e.g., Top Secret to Unclassified).

(~~S//REL TO USA, FVEY~~) **Finding** Agency CDSs

(U//~~FOUO~~) **Recommendation** Improve Agency CDS operations for all operational CDSs. **UPDATE:** A solution is in development. This recommendation remains OPEN.

(U) **Audit of Mission Assurance Continuity of Operations Compliance and Testing** (17 August 2010)

(U//~~FOUO~~) In August 2008, NSA identified 14 Mission Essential Functions (MEFs) that must be performed in all circumstances. As of August 2009, Agency organizations had been identified as being responsible for performing essential tasks that support one or more of the 14 MEFs.

(~~C//REL TO USA, FVEY~~) **Finding** A small percentage of the organizations maintained complete, updated, and operationally tested Continuity of Operations (COOP) plans.

(U//~~FOUO~~) **Recommendation** Track organization compliance in developing complete COOP plans and performing annual updates and testing. **UPDATE:** Although only a small percentage of COOP plans have been updated and tracked, this action has been given high priority. This recommendation remains OPEN.

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(U) Ongoing Audits

(U) **NSA/CSS Wireless Networks and Devices**

(U) The audit objective is to assess Agency controls for protecting against unauthorized operation of wireless networks and devices within NSA/CSS and to assess Agency wireless implementation initiatives.

(U) **High-Performance Computing**

(U) The audit objective is to evaluate the contracting process of the High Performance Computing – Special Program Office.

(U) **Information Sharing**

(U) The audit objective is to review Agency effectiveness in sharing cyber threat and vulnerability information with other IC agencies in accordance with the Comprehensive National Cyber Initiative.

(U) **Acquisition Security Process**

(U) The audit objective is to determine whether the acquisition security process effectively and efficiently mitigates the foreign ownership, control, or influence and counterintelligence risks of Agency IT purchases.

(U) **ARCANAPUP Modernization Effort**

(U) The audit objective is to determine the effectiveness of ARCANAPUP in meeting program goals.

(U) **General Application Controls for Agency Payroll, Human Resources, and Contracting Systems**

(U) The NSA Comptroller requested that we review the Defense Civilian Payroll System, the Human Resources Management System, and the Contracting Management Information System. The audit objective is to assess the general and application controls of these systems.

(U//~~FOUO~~) [redacted] **Program** (b)(3)-P.L. 86-36

(U//~~FOUO~~) The audit objective is to determine whether the [redacted] user interface meets customer needs and whether its implementation is in compliance with Agency acquisition policies.

(U//~~FOUO~~) **NSA/CSS Compliance with the Federal Information Security Management Act (FISMA)**

(U) In accordance with Office of Management and Budget guidance, we will assess the overall effectiveness of Agency information security policies, procedures, and practices. Our report will be forwarded to the ODNI Inspector General for consolidation and reporting to legislative committees.

(U) **Price Reasonableness Determinations for Agency Contracts**

(U//~~FOUO~~) The audit objective is to determine whether the Directorate of Acquisition complies with Federal Acquisition Regulation requirements for determining price reasonableness and NSA/CSS Policy 8-4, *Competition in Contracting*.

(U//~~FOUO~~) **The** [redacted] **Program**

(U//~~FOUO~~) The audit objective is to assess the privacy of data collected by [redacted] and validate that Personally Identifiable Information is adequately safeguarded from unauthorized access.

(U) **Export Controls**

(U//~~FOUO~~) The audit objective is to determine whether NSA's export control process complies with laws, regulations, and authorities.

(U) This page intentionally left blank.

(U) INSPECTIONS

(U) Inspections Completed in the Reporting Period

(U) **Joint Inspection of NSA/CSS Hawaii (NSAH)** (29 April 2011)

(U//~~FOUO~~) This inspection was conducted from 24 January to 4 February 2011. The site is led by a commander who emphasizes integration and collaboration with the Service Cryptologic Component commanders. The workforce is generally positive toward mission, but some are dissatisfied with the watch schedule, ineffective communication s across the chain of command, and the overwhelming and conflicting nature of dual responsibilities (i.e., Joint and Service). Site leadership is heavily engaged in the simultaneous transitions of host responsibilities to NSA/CSS and mission to a new building, causing gaps in mission expertise. Lack of a comprehensive financial picture and centralized manpower-tracking tools inhibits efficient use of resources and affects numerous programs that require accurate manpower and resource data,

(U) **Joint Inspection of NSA/CSS**

(U//~~FOUO~~) This inspection was conducted from 2 to 13 May 2011. NSA/CSS and enabling organizations located at the are challenged with a Staffing is adequate to meet responsibilities, although competing priorities at times stretch the staff to their limits. Military/civilian relationships are good, and the enabling organizations are customer focused. The overall climate is positive.

(U//~~FOUO~~) is focused on mission success. However, there are a number of quality-of-life challenges, ranging from facilities conditions to limited work space to distant support services.

(U//~~FOUO~~) has strong leadership that has made positive improvements to morale. The command climate at is strong. There is a clear understanding of the mission, and military/civilian relationships are positive. The Director, although relatively new, has had a positive effect on the site and projects a clear vision of where must go in the future. He has been a catalyst for positive change.

(U) **Expeditionary Operations Review (EOR) of** (28 September 2011)

(U//~~FOUO~~) The EOR Team reviewed mission operations and IO at

(b)(3)-P.L. 86-36

(~~S//REL TO USA, FVEY~~) The CST and CSGs work closely with their customers and the extended enterprise to anticipate, identify, and satisfy support requirements. Knowledgeable customers understand the contribution of Signals Intelligence (SIGINT) to operations and point to individual and team behaviors when evaluating the success of CSGs or CSTs.

(U//~~FOUO~~) Site mission, functions, tasks, authorities, and differentiation from supported commands' organic SIGINT resources must be documented, and NSA/CSS Washington must provide reporting and sanitization Standard Operating Procedures. NSA/CSS should determine the feasibility of participating in supported element pre-deployment exercises and obtain supported commands' post-deployment feedback.

(U//~~FOUO~~) IO training and database access must be included on the deployment checklist. Officers in Charge need better guidance on how to perform O functions, and guides that detail processes and procedures must be developed.

(U) Significant Recommendations Outstanding from Previous Semi-Annual Reports

(b)(3)-P.L. 86-36

(U) **Joint Inspection of** (17 November 2008)

(U) **FINDING: Fire Suppression System Lacking.**

(U//~~FOUO~~) Lack of a fire suppression system in seriously degrades the ability to protect life and critical equipment. This deficiency was initially identified during a joint Inspector General inspection and was noted again in an NSA Occupational Health and Environmental Survey. Overall stewardship of facilities is the responsibility of Planning for fire suppression system installation however, no stakeholder agencies committed the needed funding. Although it remained a critical safety deficiency, no further progress was made until the Director, NSA emphasized the need to complete the action. contracted for system design, followed by a phased installation using consolidated cryptologic program funding. A projected completion date of remains tentative because of and possible delays in getting supplies needed to complete the installation. **UPDATE:** The projected completion date is still Disruption of supplies was minimal, and the contractor made changes to the work schedule to compensate for delays.

(U) **Multiple Joint Inspections from FY2005 to FY2010 Regarding USSID CR1200**

(~~C//REL TO USA, FVEY~~) USSID CR1200, *Concept of SIGINT Support to Military Commanders*, provides policy and guidance on SIGINT support to military commanders and operations. Published in 1998, this United States Signals Intelligence Directive (USSID) is severely outdated, contains obsolete functions and terminology not used in current military doctrine, provides no Higher Headquarters template for present-day Military Operations Integration, and does not establish standards for expeditionary SIGINT support for ongoing military operations. This significant deficiency was noted as a finding in inspection reports encompassing Global Cryptologic Enterprise Sites beginning in FY2005 and continuing to the present. An NSA/CSS action element is leading a working group with stakeholder participation to draft a new USSID as recommended in this inspection report. The action element determined that other supporting policy documents must first be updated; there is no estimated

(b)(1)
(b)(3)-P.L. 86-36

completion date for this critical document. **UPDATE:** SID is developing a plan but intends to cancel this USSID. This recommendation remains OPEN.

(U) Ongoing Inspections

(U//~~FOUO~~) **Joint Inspection of**

(U//~~FOUO~~)

(U) **Joint Inspection of**

(U//~~FOUO~~) The NSA/CSS Office of Inspections conducted a Joint Inspection of The final report is in coordination.

(b) (3) -P.L. 86-36

(U) This page intentionally left blank.

(U) SPECIAL STUDIES

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) Special Studies Completed in the Reporting Period

(b) (1)
(b) (3)-P.L. 86-36

(~~TS//SI//NF~~) **NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Pen Register and Trap and Trace (PR/TT) Devices** (15 April 2011)

(~~TS//SI//NF~~) This review was conducted to determine whether the controls tested as part of a 2010 year-long review of NSA compliance with seven provisions of the Business Records (BR) Order were adequate to provide reasonable assurance of compliance with similar provisions of the PR/TT Order. Of the [redacted] queries made between [redacted] the date when the FISC signed PR/TT [redacted] and [redacted] no errors or instances of non-compliance were found with the five provisions of the PR/TT Order related to querying that were tested. These controls therefore were judged to be adequate to provide reasonable assurance of compliance with the Order. Although we intended to test NSA compliance with two additional provisions related to dissemination, we were not able to because NSA did not issue serialized SIGINT reports that contained PR/TT-derived [redacted] during the test period.

(~~TS//SI//NF~~) **NSA Controls to Comply with the FISC Order Regarding Business Records** (25 May 2011)

(~~TS//SI//NF~~) This report summarizes the results of our audit of NSA controls to comply with the FISC BR Order. From January through December 2010, we conducted monthly tests of NSA compliance with seven provisions of the BR Order to determine whether controls were in place and operating as intended. Querying controls were adequate to provide reasonable assurance of compliance with the five provisions of the Order we tested. Manual controls over the dissemination of serialized SIGINT reports and the compilation of the Weekly Dissemination Report were inherently risky but manageable. The manual dissemination controls will be increasingly difficult to manage if the amount of information disseminated outside NSA increases.

(U) **Review of Attrition of** [redacted] (26 May 2011)

(~~U//FOUO~~) The Director, NSA requested that the OIG review factors influencing recent attrition of [redacted] Between February and March 2011, the [redacted] resigned in lieu of termination on [redacted] The [redacted] were considered important to [redacted] mission because it takes [redacted] to train a replacement capable of performing at the level of those who have left. However, the overall mission impact of the departed [redacted] was considered minimal and under control. To mitigate future loss of these [redacted] the [redacted] with Human Resources assistance, is considering awarding retention bonuses to ensure that the Agency receives a return on its investment.

(b) (6)

(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(~~TS//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

(~~TS//SI//REL TO USA, FVEY~~)

(U//~~FOUO~~) **Non-Traditional Dissemination Methods: Dissemination Strategy Evaluation** (28 September 2011)

(U//~~FOUO~~) Various non-traditional dissemination methods have been implemented to address the challenges and opportunities presented by a Presidential call for increased information sharing. The review, which focused on select processes and tools that analysts use for non-traditional dissemination, revealed that SID does not have a comprehensive dissemination plan.

(U) Significant Recommendations Outstanding from Previous Semi-Annual Reports

(U) **Data Sharing with Third-Party Partners**

(U//~~FOUO~~) NSA's Third Party partners are nations other than Australia, Canada, New Zealand, and the United Kingdom with which the U.S. government has national SIGINT arrangements. The purpose of the review was to determine whether policies and procedures are in place to ensure compliance with authorities for sharing with Third-Party partners.

(U//~~FOUO~~) **Finding** Documentation for disseminated to Third Party partners is not centrally maintained, retrievable, or current.

(U//~~FOUO~~) **Recommendation** The Foreign Affairs Directorate (FAD) should establish a repository for documentation of shared with Third-Party partners and add this as a Director of Foreign Affairs responsibility in NSA/CSS Policy 10-1. **UPDATE:** FAD has established a repository but has not updated documentation. FAD has been asked to update NSA/CSS Policy 1-10 with the statement that the Foreign Affairs Director shall maintain a central repository on its database system for Third-Party information.

(~~C//REL TO USA, FVEY~~) **Finding** SID's dissemination of to Third-Party partners lacks adequate controls.

(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) **Recommendation** Review and revise the 2007 oversight process for disseminating [redacted] to partners, including sampling procedures. Inform the workforce of the revised process.

(~~S//NF~~) **Recommendation** Establish a standard process for handling all [redacted] **UPDATE:** SID has developed a process but has not formally approved or communicated it to the workforce.

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) After the 11 September 2001 terrorist attacks on the United States, NSA established a [redacted] Since then, [redacted] has undergone several reorganizations; most recently, [redacted] became an element of the SIGINT Development Strategy and Governance organization.

(U//~~FOUO~~) **Finding** [redacted] lacks essential authorizing mission documentation and standards.

(~~C//REL TO USA, FVEY~~) **Recommendation** Publish and publicize the missions and functions of [redacted] field sites, clearly defining the division of effort, prioritization, measures of success, and roles and responsibilities of personnel. **UPDATE:** [redacted] is making slow progress.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) **Finding** [redacted] lacks an IO program.

(U//~~FOUO~~) **Recommendation** Designate an [redacted] IO Officer focused on IO standards and practices to establish an [redacted] SOP that clearly delineates the standards for accepting, loading, processing, storing, reporting, and querying data associated with U.S. persons in accordance with DoD Regulation 5240.1-R and other regulations and instructions. **UPDATE:** [redacted] is making slow progress.

(U) Ongoing Special Studies

(U//~~FOUO~~) **Management Controls to Implement the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008**

(U//~~FOUO~~) The objective of this study is to determine whether NSA controls are adequate to provide reasonable assurance that NSA complies with the terms of the FISA Amendments Act.

(U//~~FOUO~~) **Computer Network Exploitation by** [redacted]

(U//~~FOUO~~) The objective of this study is to evaluate [redacted] FISA operations for compliance with national and NSA policies and procedures.

(~~TS//SI//NF~~) **NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Retention**

(~~TS//SI//NF~~) The objective of this study is to determine whether NSA controls are adequate to provide reasonable assurance that NSA complies with the terms of the FISC Order for BR retention.

(U) [redacted]

(~~S//SI//REL TO USA, FVEY~~) The objective of this study is to review recent [redacted]

[redacted]

(b) (1)
(b) (3)-P.L. 86-36

(U) This page intentionally left blank.

(U) INVESTIGATIONS

(U) Summary of Prosecutions

(U) Indictment

(U) In May 2011, a federal grand jury indicted three family members for conspiracy to commit wire fraud arising from a fraudulent billing scheme on an NSA contract. The defendants, all former officials of an Agency contractor, are alleged to have instructed employees to inflate the number of hours spent working on NSA contracts and, in some cases, to claim time spent working on NSA contracts when in fact they had not been. The indictment seeks forfeiture of $1,455,174, believed to be the amount of payments fraudulently received from NSA.

(U) Sentencing

(U) In June 2011, a former Agency employee was sentenced to 18 months in prison followed by three years of supervised release for conspiring to obtain payments in return for taking actions as an NSA official and for making false statements to conceal the illegal payments from the Agency. The former employee was also ordered to serve six months of the supervised release in home detention with electronic monitoring and to perform 100 hours of community service and pay a $15,000 fine and $4,929.90 in restitution within 60 days. In the same case, two officials in a private company, who had made the improper payments, were also sentenced: one to one year and one day incarceration and three years of supervised release and the other to six months in prison followed by one year of supervised release. The company was also ordered to pay a fine of $130,000 and restitution of $104,989.84 (which has been paid in full).

(U) In September 2011, a former NSA contractor employee was sentenced to five years of probation, ten months of which is to be served in home detention with electronic monitoring, for making false statements in connection with labor hours claimed on an NSA contract. The former contractor employee was also required to pay restitution of $108,780.46, which represents payment for 836 labor hours not actually performed.

(U) Referrals

(U) The U.S. Attorney's Office in Baltimore, Maryland, is considering a contract labor mischarging case. The dollar amount is approximately $49,000, representing approximately 677 falsely claimed labor hours.

(U) OIG Hotline Activity

(U) The division fielded 571 contacts from the OIG Hotline. The team opened 53 investigations and closed 46 in the reporting period.

(U) This page intentionally left blank.

(U) INDEX OF REPORTING REQUIREMENTS

(U)

IG Act	Reporting Requirement	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	1-2
§5(a)(2)	Recommendations for corrective action	1-2
§5(a)(3)	Previously reported significant recommendations not yet completed	4, 8-9, 12-13
§5(a)(4)	Matters referred to prosecutive authorities	15
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	19
§5(a)(7)	Summary of significant reports	1-2
§5(a)(8)	Audit reports with questioned costs	21
§5(a)(9)	Audit reports with funds that could be put to better use	23
§5(a)(10)	Summary of reports for which no management decision was made	N/A
§5(a)(11)	Significant revised management decisions	N/A
§5(a)(12)	Management decision disagreements	N/A

(U)

(U) This page intentionally left blank.

(U) APPENDIX A: AUDITS, INSPECTIONS, AND SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD

(U) Audits

(U) **Information Technology**

- (U) Agency Controls for [redacted] IT Hardware Purchases
- (U) Nuclear Command and Control

(U) **Federal Compliance**

- NSA/CSS Compliance with the Federal Information Security Management Act (FISMA)

(U) **Operations**

- (U) NSA Police Operations

(U) Inspections

(U) **Joint Inspections**

- (U) NSA/CSS Hawaii

(U//~~FOUO~~) (U) NSA/CSS Europe, [redacted]

(U) **Operations**

- (U) Expeditionary Operations Review of [redacted]

(U) Special Studies

(U) **Operations**

- (U) Review of Attrition of [redacted]
- (~~TS//SI//REL TO USA, FVEY~~) [redacted]
- (~~TS//SI//REL TO USA, FVEY~~) [redacted]

(U) **Intelligence Oversight**

- (~~TS//SI//NF~~) NSA Controls to Comply with the Foreign Intelligence Surveillance Court (FISC) Order Regarding Pen Register and Trap and Trace Devices
- (~~TS//SI//NF~~) NSA Controls to Comply with the FISC Order Regarding Business Records

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) APPENDIX B:
AUDIT REPORTS WITH QUESTIONED COSTS

(U)

Report	Number	Questioned Costs	Unsupported Costs
For which no management decision had been made by start of reporting period	0	0	0
Issued during reporting period	0	0	0
For which management decision was made during reporting period	0	0	0
Costs disallowed	0	0	0
Costs not disallowed	0	0	0
For which no management decision was made by end of reporting period	0	0	0
(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.			

(U)

(U) This page intentionally left blank.

(U) APPENDIX C:
AUDIT REPORTS OF FUNDS THAT COULD BE PUT TO BETTER USE

(U)

Report	Number	Amount
For which no management decision had been made by start of reporting period	0	0
Issued during reporting period	1	$491,400 over 5-yr defense plan
For which management decision was made during reporting period	1	$491,400 over 5-yr defense plan
Value of recommendations agreed to by management	1	$466,602 over 5-yr defense plan
Value of recommendations not agreed to by management	1	$24,798 over 5-yr defense plan
For which no management decision was made by end of reporting period	0	0
(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.		

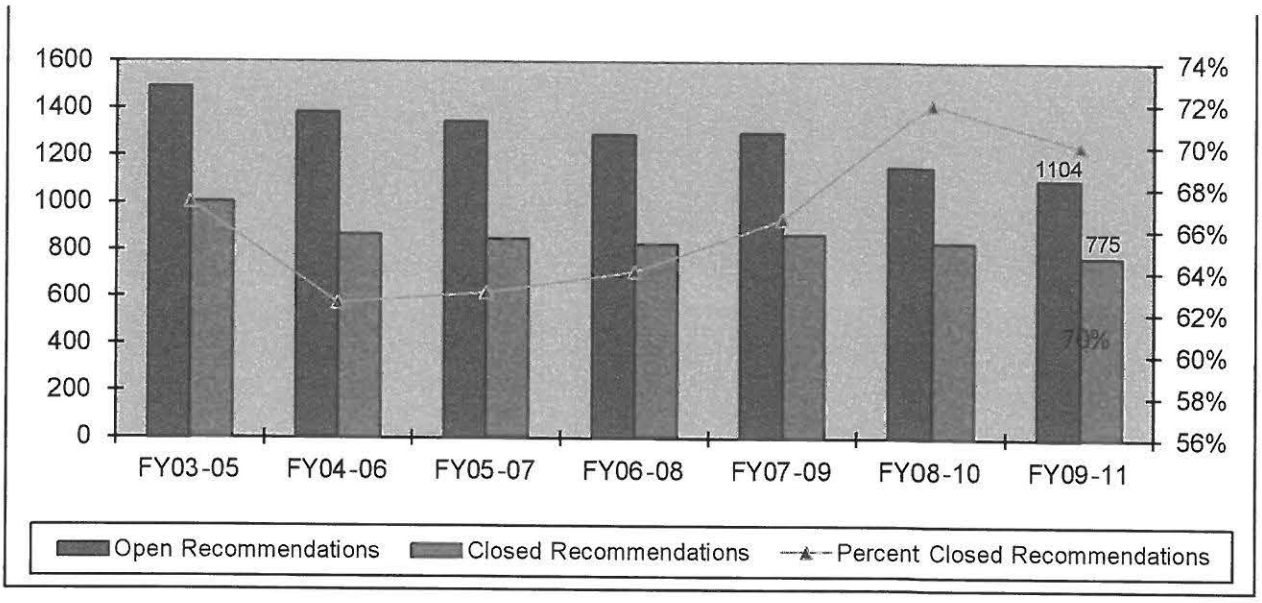
(U)

(U) This page intentionally left blank.

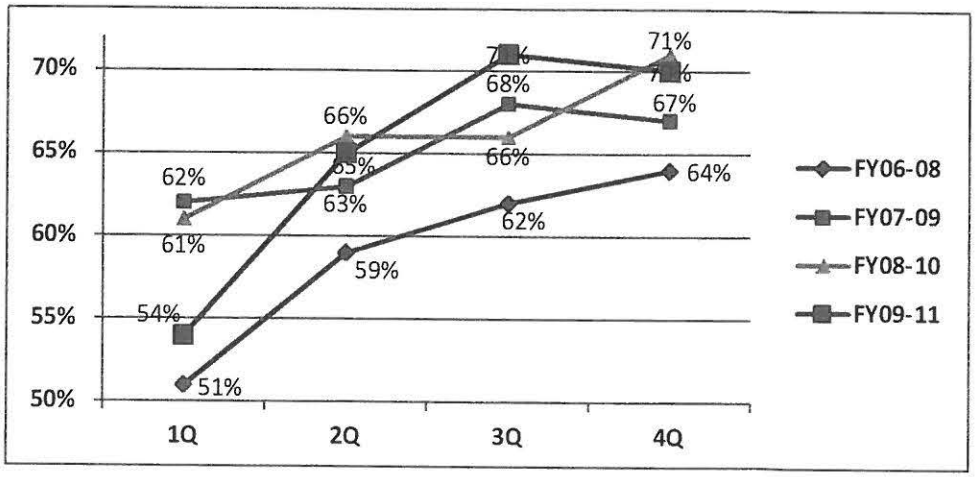
(U) APPENDIX D: RECOMMENDATIONS SUMMARY

(U//~~FOUO~~) The OIG made 213 new recommendations to NSA management in reports issued in the third and fourth quarters of FY2011: 99 in the third and 114 in the fourth. During the third and fourth quarters, the Agency implemented 84 and 71 recommendations, respectively. Figures 1 and 2 depict long-term progress in implementing OIG recommendations. We monitor recommendation completion on a rolling three-year average.

(U) Figure 1. Agency Implementation of OIG Recommendations



(U) Figure 2. Implementation Rate Comparison



(U) Percentages depict progress in implementing recommendations during a three-year period by quarter. Progress in the fourth quarter during the current three-year period is consistent with historical norms.

(b)(3)-P.L. 86-36

(U) Highlights

(U//~~FOUO~~) Managers fully implemented recommendations made in the following reports by the end of the fourth quarter:

- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) Package Screening for Chemical & Biological Agents (31 March 2006)
- (U//~~FOUO~~) NSA's Computer Security Incident Response Process (26 September 2006)
- (U) SPL Mask-Making and Wafer Fabrication Closeout (23 June 2008)
- (U) Agency System Security Plans (8 September 2008)
- (U) FMS FACTS (31 December 2008)
- (U) NSA/CSS Threat Operations Center (31 March 2009)
- (U) NSA/CSS Commercial Solutions Center (28 August 2009)
- (~~S//REL TO USA, FVEY~~) [redacted]
- (U) Foreign Language Incentive Program (13 May 2009)
- (~~TS//REL TO USA, FVEY~~) [redacted] (25 September 2009)
- (~~TS//REL TO USA, FVEY~~) [redacted] (25 September 2009)
- (U) Follow-up Audit of Contractor Space (30 September 2009)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) *For the Period April 1, 2009 through September 30, 2009*

(U//~~FOUO~~) **Foreign Language Incentive Pay Program**; NSA/CSS IG; ST-09-0005; 13 May 2009

(U//~~FOUO~~) **Summary** A special study found that the Foreign Language Incentive Pay (FLIP) program does not always meet its goals of encouraging civilian Language Analysts (LA) to acquire and maintain language skills and influencing them to remain in language analysis positions. [redacted] Since the implementation of the Defense Language Proficiency Test (DLPT [redacted] the DoD standard, language readiness for [redacted] for which the [redacted] is the test of record. [redacted] the Agency's investment in the FLIP program, which increased from [redacted] in FY06 to [redacted] in FY07. Although the annual FLIP validation process is working well, FLIP management controls are weak.

(U) **Management Action** The NSA CoS has begun to take action on the recommendation for a program review in which the Signals Intelligence Directorate will participate.

(U) **Overall Report Classification** SECRET//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **NSA/CSS Texas**; NSA/CSS IG; AFISRA IG; INSCOM IG; NNWC IG; JT-09-0002; 1 July 2009

(~~S//REL TO USA, FVEY~~) **Summary** The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency, Intelligence and Security Command, Naval Network Warfare Command, and NSA inspected NSA/CSS Texas (NSAT). Since a 2006 inspection, NSAT has taken on additional global missions such as [redacted] while broadening the scope of others, including [redacted] and Customer Relations. Several responsibilities, such [redacted] have transferred to other sites. Key points from the inspection include: 1) NSA HQ/Signals Intelligence Directorate has delegated mission to NSAT [redacted] 2) NSAT leadership has been effective in [redacted]

(U) **Management Action** Management concurred with all recommendations and corrective actions are underway.

(U) **Overall Report Classification** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

(b)(1)
(b)(3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~*20320108*~~

(b)(3)-P.L. 86-36

(U) **Interim Report of NSA/CSS on Mission Assurance**; NSA/CSS IG; IN-09-0003; 8 July 2009

~~(S//REL TO USA, FVEY)~~ **Summary** The OIG's inspection of mission assurance provided background on implementation of the mission assurance policy objectives and addressed the organizational placement of the Agency's Enterprise Mission Assurance (EMA) function. Placement of EMA within the [redacted] is inconsistent with EMA's corporate responsibilities outlined in NSA/CSS Policy 1-4, *Mission Assurance* (1 February 2006). The consensus among the senior leaders was that [redacted] would be a more appropriate site for EMA [redacted] The inspection also found that some progress has been made on several Policy 1-4 objectives; however, [redacted]

(U//~~FOUO~~) **Management Action** EMA was transferred [redacted] EMA [redacted] will continue to collaborate with the Technology Directorate to [redacted] and embed mission assurance principles in governance, planning, and acquisition programs. The goal of both organizations is to ensure that the nation's SIGINT and Information Assurance missions will continue to operate through any disruption.

(U) **Overall Report Classification** SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

(b)(1)
(b)(3)-P.L. 86-36

~~(S)~~ **OIG Inquiry into the Red Team [redacted] Incident**; NSA/CSS IG; [redacted]

~~(S//REL)~~ **Summary** The objectives of the inquiry were to establish the facts surrounding the incident, evaluate responsibility, and assess compliance with internal controls and their adequacy for preventing future incidents. The inquiry found that Red Team controls were not adequate to prevent the human errors [redacted] had discontinued the [redacted] when problems became evident. Poor communication between Red Teams and with Red Team Operations Management contributed to the incidents. Although human error caused the [redacted] Red Team managers are responsible for the control environment in which the errors occurred.

~~(S//REL)~~ **Management Action** In response to our inquiry, Red Teams stopped [redacted] pending approval to resume, stopped operations, and removed Red Team personnel from [redacted] to ensure data integrity. Red Team management updated training processes and materials and conducted a training "stand-down" to ensure that all employees understood Standard Operating Procedures and policies. Red Team management is re-emphasizing and clarifying responsibilities to minimize the likelihood of recurrence. Information Assurance Directorate management concurs with the findings and has begun corrective action.

(U) **Overall Report Classification** SECRET//REL TO USA, FVEY

(U) **Category** Information Security and Privacy

(U//~~FOUO~~) **FY2009 Audit Report on Compliance with the Federal Information Security Management Act at NSA/CSS**; NSA/CSS IG; AU-09-00011; 24 July 2009

(U//~~FOUO~~) **Summary** The Agency's emerging mission in the Comprehensive National Cybersecurity Initiative (CNCI) depends, in part, on the Agency's ability to protect its systems and networks. The Federal Information Security Management Act (FISMA) measures the adequacy and effectiveness of the information security environment upon which this emerging mission is based. The FY2009 FISMA Report records the progress the Agency has made in strengthening information technology (IT) security processes and in tracking Agency-wide and system deficiencies. However, more work must be done to correct the material weakness reported in August 2006 regarding [redacted] the NSA/CSS Information Systems Incident Response Team developed a formal follow-up system for [redacted] and Contractor Accreditations and Inspections continues to meet a self-initiated goal of [redacted]

(U) **Management Action** Management concurred with all recommendations, and corrective actions are underway.

(U) **Overall Report Classification** TOP SECRET//COMINT//NOFORN (b)(3)-P.L. 86-36

(U) **Category** Information Security and Privacy

(U//~~FOUO~~) **Audit of Associate Directorate for Education and Training Information Technology Infrastructure Problems**; NSA/CSS IG; AU-09-0019; 28 July 2009

(U//~~FOUO~~) **Summary** The principal audit objective was to determine whether the Associate Directorate for Education and Training (ADET) IT servers are adequately controlled and operated in accordance with guidelines, policies, and regulations. [redacted] ADET experienced a significant server crash when [redacted] The audit found that [redacted] contributed to this problem. The incident highlighted the need for ADET to bring the [redacted] into compliance with the certification and accreditation process.

(U//~~FOUO~~) **Management Action** Action is underway to rebuild and restore approximately [redacted] web pages and [redacted] applications that were lost at an estimated cost of [redacted] To facilitate improvements in the VUport infrastructure, ADET has requested the expertise of the Technology Directorate (TD) and is considering transferring its systems management to TD. The OIG recommended that ADET ensure that [redacted] comply with the certification and accreditation process. ADET agreed to do so by 30 September 2009.

(U) **Overall Report Classification** TOP SECRET//COMINT/TALENT KEYHOLE//REL TO USA, FVEY

(U) **Category** Information Security and Privacy

(U//~~FOUO~~) **Advisory Audit Report on Strengthening Contract Administration to Protect Agency Resources**; NSA/CSS IG; AU-09-0001; 6 August 2009

(U//~~FOUO~~) **Summary** Contract administration has been a longstanding problem at NSA. Over the last decade, the OIG reported contract administration problems in 65 audit, investigation, and inspection reports. Yet deficiencies addressed in one report almost invariably recur in the next. These deficiencies included inadequate invoice certification, out-of-scope work, award fee contract administration deficiencies, and other oversight concerns. These weaknesses were caused by inadequate training, over-reliance on contractors, and failure to follow policies and procedures. A powerful example of the consequences of poor contract administration can be seen in the OIG's ongoing effort to uncover contract labor mischarging. To date, recoveries from fraudulent billings or out-of-scope work exceed $1.4 million. The advisory audit found that, although recent initiatives to address staffing shortages and reform policies have produced some improvement, the Agency must develop a comprehensive and consistent approach to correct these deficiencies. Contracting Officers and contracting specialists reported in two OIG surveys that they do not have time to perform contract administration adequately. The OIG proposed that the Senior Acquisition Executive with the Senior Leadership Team establish a contract administration process within the Directorate of Acquisition to provide adequate contract management, including oversight of Contracting Officer's Representatives.

(U) **Overall Report Classification** SECRET//REL TO USA, FVEY

(U) **Category** Acquisition Processes and Contract Management

(U//~~FOUO~~) **Report of Investigation Regarding Alleged Improprieties at NSA Georgia**; NSA/CSS IG; IV-09-0003; 14 August 2009

(U//~~FOUO~~) **Summary** A former Navy linguist [redacted] at NSA/CSS Georgia (NSAG) from 2004 until 2007 alleged that the [redacted] program at NSAG had unlawfully intercepted and processed U.S. person communications. [redacted]

~~(S//REL TO USA, FVEY)~~ The OIG found no targeting of U.S. persons by [redacted]. The investigation involved [redacted] interviews of the complainant, more than [redacted] witness interviews, [redacted] and the forensic analysis of [redacted] records. Analysis showed that [redacted] handled approximately [redacted] during the period the complainant's allegation covered (2004-2005) and that [redacted] (.022 percent) [redacted] were incidentally collected U.S. communications. [redacted] Incidental collection of U.S. person communications is a by-product of collection against legitimate foreign targets. The forensic data and relevant testimony showed that [redacted] personnel handled incidentally collected U.S. person communications in accordance

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

with USSID SP0018, marking and deleting them as appropriate.

(U//~~FOUO~~) The complainant also alleged that, solely for entertainment purposes, [redacted] had shared [redacted] The OIG found no merit to this allegation. [redacted]

(U//~~FOUO~~) The complainant also made two allegations regarding unlawful activity involving [redacted] The OIG investigation determined that these allegations were without merit.

(U) **Overall Report Classification** TOP SECRET//COMINT//NOFORN

(U) **Category** Questionable Activities

(b)(3)-P.L. 86-36

(U) **NSA/CSS Commercial Solutions Center**; NSA/CSS IG; IN-09-0002; 27 August 2009

(U//~~FOUO~~) **Summary** The NSA/CSS Commercial Solutions Center (NCSC) is meeting its customers' needs and succeeding in its role as the NSA front door for industry partners. Overall, NCSC [redacted] The NCSC has adequate information to manage its annual budget and predict anticipated funds for the following year. Some senior Agency leadership, especially from the Signals Intelligence Directorate (SID), believe that the NCSC would be more effective if its functions were moved into SID. The OIG inspection found no evidence to support this assertion. Although NCSC is achieving its mission well, the inspection revealed the need for: 1) comprehensive training for platform managers, whose role is critical to NCSC success, 2) an overarching acquisition strategy for Consolidated Cryptologic Program procurements that exceed [redacted] and 3) changes to the current Issue Resolution Process to ensure compliance with NSA/CSS Policy 3-13 guidance to disseminate information technology vulnerability alerts quickly.

(U) **Management Action** NCSC and SID management concurred on the recommendations.

(U) **Overall Report Classification** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Acquisition Processes and Contract Management

(U) [redacted] NSA/CSS IG; IN-09-0005;

~~(S//REL TO USA, FVEY)~~ **Summary** The inspection found that the [redacted] suffers from lack of strategic direction because of uncertainty surrounding [redacted] The site's motivated workforce and strong leadership need [redacted] to achieve the [redacted] full potential [redacted] The inspection revealed

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

~~SECRET//REL TO USA, FVEY~~

management controls in need of improvement. The current NSA/CSS [redacted] The site's resource alignment must be evaluated regularly in light of the disappointing results. The site lacks a vetting process and tracking system to oversee its requests.

(U) **Management Action** [redacted] and associated Agency elements concurred on all recommendations and are taking corrective action.

(U) **Overall Report Classification** SECRET//COMINT//NOFORN

(U) **Category** Joint Warfighting and Readiness

(U) **Federally Funded Research and Development Center – Institute for Defense Analyses**; NSA/CSS IG; AU-08-0008; 16 September 2009

(U//~~FOUO~~) **Summary** The principal audit objective was to determine whether the Institute for Defense Analyses (IDA) contract is being administered effectively and in compliance with contracting and information systems security policies and procedures. The long term research partnership with IDA has yielded many Signals Intelligence and Information Assurance successes. However, our audit found that [redacted] Officer's Representative is also needed to determine compliance with contracts, effectiveness of internal controls, and the cost efficiency of operations.

(U) **Management Action** The Technology and Acquisition Directorates, in conjunction with the Office of Mathematics Research Contracting Officer Representative, has initiated action on all OIG recommendations.

(U) **Overall Report Classification** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Acquisition Processes and Contract Management (b) (3)-P.L. 86-36

(U//~~FOUO~~) [redacted] NSA/CSS IG;AFISRA IG; INSCOM IG; NNWC IG; [redacted] 16 September 2009

~~(S//REL TO USA, FVEY)~~ **Summary** The Inspectors General from the National Security Agency, Air Force Intelligence, Surveillance and Reconnaissance Agency, Army Intelligence and Security Command, and Naval Network Warfare Command conducted a joint inspection of the [redacted] which is jointly managed and has been an exemplar of First and Second Party mission partner collaboration [redacted] The diversity of the mission partners working with full knowledge of all missions at [redacted] is both a strength and a burden. This [redacted] environment is key to the superior collaboration at site, but it is cumbersome when sharable information and tools reside on NOFORN and other systems. Personnel external to the site must be educated to understand site restrictions and proper classification to enable tools and information sharing. [redacted]

(b) (1)
(b) (3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

[redacted]

(U) **Management Action** Management concurred with all recommendations, and corrective actions are underway.

(U) **Overall Report Classification** SECRET//COMINT//TALENT KEYHOLE//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

(U) **Follow-up Audit of Contractor Space**; NSA/CSS IG; AU-08-0020; 30 September 2009

(U//~~FOUO~~) **Summary** Since 2003, NSA has tried unsuccessfully to alleviate chronic shortages of space by targeting increasing use of government space by contractors. The effort included contractor relocation, a restrictive contractor occupancy policy, and industry sponsored facilities. Although recommendations from a 2004 audit have been implemented, management of contractor space remains a significant problem. Our follow-up audit [redacted]

[redacted]

(U) **Management Action** Management concurred with all recommendations.

(U) **Overall Report Classification** SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Human Capital

(U) **False Contractor Labor Claims**; NSA/CSS IG; IV-07-0031, IV-08-0016, IV-08-0017, IV-08-0018, IV-08-0019; 13 March 2009 – 12 August 2009

(U//~~FOUO~~) **Summary** Between 2004 and 2007, five contractors working the midnight shift on an Agency in-house contract submitted false and inaccurate timesheets to their companies. All five took days off and covered for each other, while claiming 8-hour shifts on their timesheets. Since they were working on a time and materials contract, the government was over-billed approximately $116,000 as a result of this fraud. All the contractors have left their companies and no longer work on NSA contracts. The most egregious offender pled guilty to three counts of violating 18 U.S.C. Section 1001 (False Statements) and was sentenced to 30 days in prison and two years supervised release. The individual was also ordered to pay restitution of nearly $75,000.

(U) **Management Action** The Office of Contracting and the prime contractor have been notified of the results of the investigation to facilitate monetary recovery.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Procurement and Contract Administration)

(U) **Time Card Fraud**; NSA/CSS IG; IV-08-0004; 1 September 2009

(U//~~FOUO~~) **Summary** A GG-14 employee knowingly submitted falsified time sheets from August 2006 to January 2008 for a shortfall to the Government of 615.25 hours (approximately $34,059).

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Standards of Conduct)

(U) **Procurement Fraud Initiative**; NSA/CSS IG; Several Control Numbers; 1 April 2009 to 30 September 2009

(U//~~FOUO~~) **IV-09-0015** A contractor employee fraudulently billed the government 525 hours (approximately $58,000) over 14 months for late arrivals, early departures, and long lunches. The employee was terminated by the contractor during our investigation.

(U//~~FOUO~~) **IV-09-0024** A major contractor has a policy which directs employees to bill indirect time "under 59 minutes" to contracts instead of overhead. The OIG is coordinating a review with DCAA regarding this practice. The practice was discovered during an investigation of an employee who had billed Agency contracts 57 hours over 12 months for "overhead activities," such as reading company email or completing timesheets.

(U//~~FOUO~~) **IV-09-0026** A contractor employee fraudulently billed the government 117.5 hours (approximately $14,000) over 12 months.

(U//~~FOUO~~) **IV-09-0031** A contractor employee fraudulently billed the government 502 hours (approximately $85,000) over 19 months.

(U//~~FOUO~~) The OIG is continuing to investigat e mischarging at cryptologic centers. Ten investigations are open for contract labor mischarging at the Hawaii site. The initial estimate of mischarging for these employees is almost $400,000.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Procurement and Contract Administration)

~~SECRET//REL TO USA, FVEY~~

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U//~~FOUO~~) NSA/CSS IG;

~~(S//REL)~~ **Summary** The inspection of the is organized and managed to fulfill its mission requirements with few impediments. Its services are sought by customers within and outside NSA, and its products and services fight against terrorism. Based on our positive assessment of is managed, we curtailed the scope of the inspection and reported only one deficiency: divisions are capable of operating as independent entities, management has developed an organizational structure that produces an overall value greater than the sum of its parts.

(U) **Management Action** All action officials concurred with the recommendation that approval be obtained to operate the information systems.

(U) **Overall Report Classification** SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Review of the President's Surveillance Program**; NSA/CSS IG; ST-09-0002; 29 June 2009

~~(S//REL)~~ **Summary** In response to a provision of the FISA Amendments Act of 2008, the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and the Central Intelligence Agency completed a comprehensive review of the President's Surveillance Program that included, in accordance with the legislation, a description of: (A) all facts necessary to describe the establishment, implementation, product, and use of the product of the Program; (B) access to legal reviews of the Program and information about the Program; (C) communications with, and participation of, individuals and entities in the private sector related to the Program; (D) interaction with the Foreign Intelligence Surveillance Court and transition to court orders related to the Program; and (E) other matters necessary for a complete a review of the Program. An unclassified report, a classified capstone report, NSA's individual classified report, and the classified reports of the other four OIGs were delivered to the Senate and House Intelligence Oversight and Judiciary committees in July 2009.

(U) **Overall Report Classification** TOP SECRET/ /COMINT//ORCON//NOF ORN

(U) **Category** Joint Warfighting and Readiness

(b) (1)
(b) (3)-P.L. 86-36

~~SECRET//REL TO USA, FVEY~~

(b) (3)-P.L. 86-36

(U) [redacted] NSA/CSS IG; [redacted]
25 September 2009 (both reports)

(S//~~REL~~) **Summary** The OIG visited two [redacted] sites selected on the basis of risk, location, and [redacted] The reviews assessed site operations, local customer support, and compliance with intelligence oversight requirements and [redacted] Several findings and recommendations at each site addressed procedures and conditions that have arisen as a result of expanded missions of [redacted] including the need for quick computer network response time, updates to software, and accountability mechanisms. The review also made recommendations to address the implementation of the [redacted] and changes in site requirements and capabilities.

(U) **Management Action** [redacted] management at the site and [redacted] Headquarters concurred with the findings and are taking action to implement the recommendations.

(U) **Overall Report Classifications** TOP SECRET//COMINT//NOFORN [redacted]
TOP SECRET//COMINT//NOFORN [redacted]

(U) **Category** Joint Warfighting and Readiness

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) *For the Period October 1, 2008 through March 31, 2009*

(b) (3)-P.L. 86-36

(U//~~FOUO~~) NSA/CSS IG; AFISRA IG, INSCOM IG, NNWC IG,

~~(C//REL)~~ Summary The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency, Intelligence and Security Command, Naval Network Warfare Command, and NSA inspected the The team found the site led by a commander who energizes operational and enabling personnel and improved skills and tools used in the cryptologic mission. Exceptional leadership at the is reflected in the low number of findings; however, the IG team found that many problems identified in the 2005 Joint Inspectors General Inspection Report continue to reduce site effectiveness. The inspection team attributes most of these problems to the fact that there is no process for converting a Service Cryptologic Element site to an NSA/CSS field site and that there is no NSA headquarters vision for Furthermore, substandard facilities, training shortfalls, and decreasing mission support despite an increased pace of system installations can be traced to the absence of an overarching financial picture and centralized resource planning.

(U) Management Action **Management concurred with all recommendations and corrective actions are underway.**

(U) Overall Report Classifications **SECRET//COMINT//REL TO USA, FVEY**

(U) Category **Joint Warfighting and Readiness**

~~(S//REL)~~ ; NSA/CSS IG; 12 December 2008 (both reports).

~~(S//REL)~~ Summary **We visited sites selected on the basis of and reported oversight problems. Our reviews assessed site operations, and compliance with intelligence oversight requirements and instructions. We had no findings or recommendations at had not conducted an We recommended that Headquarters consider performing a**

(U) **Management Action** management at the site advised that the exercise had been conducted Headquarters is investigating

(U) Overall Report Classifications: **TOP SECRET//COMINT /NOFORN (ST-08-0012A); TOP SECRET//COMINT//NOFORN (ST-08-0012B)**

(U) Category: **Joint Warfighting and Readiness**

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(U) **Financial Accounting and Corporate Tracking System (FACTS);** NSA/CSS IG; AU-08-0019; 31 December 2008

~~(S//REL)~~ **Summary In May 2008, the House Permanent Select Committee on Intelligence requested that the NSA OIG independently review FACTS and report to the congressional intelligence committees. Originally planned for implementation in November 2004, FACTS was implemented in October 2007 after three delays. FACTS implementation has resulted in major accounting and process problems, especially in administrative control of funds, financial planning, accounts receivable, accounts payable, reconciling accounts, and cash reporting. FACTS has cost more than [redacted] to date, with another [redacted] budgeted for FY2009-2014. From the outset, FACTS [redacted]**

(U) **Management Action** Management concurred with all recommendations.

(U) Overall Report Classifications **SECRET//REL TO USA, FVEY**

(U) Category **Financial Management**

(b)(1)
(b)(3)-P.L. 86-36

(U) **Temporary Secure Work Areas;** NSA/CSS IG; ST-08-0021; 5 January 2009

(U//~~FOUO~~) **Summary This special study was initiated as a result of a complaint received by the OIG concerning the use of a facility as a non-accredited Sensitive Compartmented Information Facility (SCIF). The complainant alleged that NSA's practice of repeatedly using a certain uncleared, unsecured venue as a Temporary Secure Work Area (TSWA) places sensitive classified information at risk. Although the venue is not an accredited SCIF, it has been designated as a TSWA. The special study focused on the circumstances and implications of the Agency's designation of the facility as a TSWA and the overall TSWA approval process. NSA's Associate Directorate for Security and Counterintelligence (ADS&CI) is the Cognizant Security Authority for NSA and is responsible for security program management for the protection of sources and methods. The special study found that this matter has been researched and addressed appropriately. Furthermore, ADS&CI has complied with Director of Intelligence Directive No. 6/9, *Physical Security Standards for Sensitive Compartmented Information.***

(U) **Management Action Management concurred with our recommendation to avoid future approvals of the facility as a TSWA.**

(U) Overall Report Classifications **SECRET//NOFORN**

(U) Category **Other (Physical Security)**

(U//~~FOUO~~) **Aerospace Data Facility;** NSA/CSS IG, NGA IG, AFISRA IG, INSCOM IG, NNWC IG; JT-09-0001; 15 January 2009

(U//~~FOUO~~) **Summary The IG organizations of the National Geospatial-Intelligence Agency, Air Force Intelligence, Surveillance, and Reconnaissance Agency, Intelligence and Security Command, Naval Network Warfare Command, NSA, and other agencies conducted a joint inspection of the Aerospace Data Facility. The inspection team found the site led by a commander who energizes the operational and enabling missions. Without clear and consistent guidance from the Intelligence Community (IC), the Commander has done an exceptional job of developing and communicating vision and direction to move from agency mission stovepipes to IC-centric operations. When structured properly, the NSA, NGA, Service Cryptologic Elements, foreign mission partners, and corporate partners at the site present an ideal environment for a cohesive, collaborative relationship that supports the Director of National Intelligence's (DNI) Strategic Plan to create a culture in which intelligence professionals work together. The inspection team found that a more integrated mission environment would support the DNI's functional joint duty assignment initiative. A** [redacted] **independent site services, and agency specific rather than IC-centric processes threaten the site's ability to achieve this vision.**

(U) **Management Action Management concurred with all recommendations and corrective actions are underway.**

(b) (3)-P.L. 86-36

(U) Overall Report Classifications **TOP SECRET//COMINT//TALENT KEYHOLE//NOFORN**

(U) Category **Joint Warfighting and Readiness**

(U) **Advisory Report on Human Language Technology**; NSA/CSS IG; AU-09-0004; 4 February 2009

~~(S//REL)~~ **Summary Our advisory found that the NSA program to improve SIGINT communications processing has invested approximately** [redacted] **to date and plans to spend** [redacted] **over the FY2009 – FY2013 program build. This program, known as Human Language Technology (HLT), provides products and services to SIGINT analysts to** [redacted] **find, evaluate, and report intelligence information critical to national security. Our advisory found that collaboration between users of HLT and researchers is key to the program's success. Not all HLT programs have been successful, but knowledge has been gained from attempts that failed and those that succeeded. Nevertheless, the problem the HLT program was designed to resolve remains:** [redacted] **With limited resources, NSA must** [redacted] **that will yield the best results.**

(U) **Management Action Management has stated that over the next 15 months each HLT area will be evaluated for inclusion within the Analytic Modernization program or termination.**

(b) (1)
(b) (3)-P.L. 86-36

(U) Overall Report Classifications **TOP SECRET//COMINT//NOFORN**

(U) Category **Joint Warfighting and Readiness**

(U) **Oversight Review of Restaurant Fund, Civilian Welfare Fund, and Cryptologic**

Museum Gift Shop; NSA/CSS IG; AU-09-0017; 17 March 2009

(U//~~FOUO~~) **Summary The financial statements of the Agency's Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop were audited by a Certified Public Accounting firm which issued unqualified opinions. Our review found that the audit had been conducted consistent with Government Auditing Standards. The CPAs did not identify any management concerns in this or the previous year.**

(U) Overall Report Classifications **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

(U) Category **Financial Management**

(U) **Deployment of SIGINT Systems**; NSA/CSS IG; AU-08-0010; 27 March 2009

(U//~~FOUO~~) **Summary Our objective was to determine whether deployments of SIGINT systems and tools to the field complied with NSA policies. The Agency is generally in compliance with the process for deploying SIGINT and support capabilities to field sites.** [redacted] **of sampled NSA/CSS capabilities deployed during FY2007 and FY2008 followed or partially followed the deployment management process prescribed by NSA/CSS Policy Manual 10-4. The manual details the processes for deploying capabilities to field sites, including verifying that the capability is ready to be deployed and that the site is prepared for its installation, integration, operation, and maintenance. Although the policy manual addresses most deployment situations, some areas have been overlooked. For example, the manual and the Acquisition Logistics & Deployment Review Office web pages do not define requirements for** [redacted]

(U) **Management Action The actions taken by the Directorate of Acquisition and the Technology Directorate meet the intent of the recommendations.**

(U) Overall Report Classifications **SECRET//COMINT//TALENT KEYHOLE//REL TO USA, FVEY**

(U) Category **Joint Warfighting and Readiness**

(b)(1)
(b)(3)-P.L. 86-36

(U) **Organizational Inspection of the NSA/CSS Threat Operations Center**; NSA/CSS IG; IN-08-0004; 31 March 2009

~~(S//REL)~~ **Summary Since the inception of the NSA/CSS Threat Operations Center (NTOC) in 2005, Agency senior leadership has been unable to implement the Director's strategic intent for the organization. Our inspection found that disagreements on mission boundaries have prevented NTOC from establishing the foundation required to perform its mission. Recognizing cyber security as a significant national security challenge, the Director NSA/CSS (DIRNSA) established the NTOC as a corporate organization to maximize the Signals Intelligence (SID) and Information Assurance Directorates' (IAD) computer network operations capabilities. DIRNSA has provided much of the guidance on NTOC's strategic mission to the NTOC Director; some of that guidance has conflicted with the established missions of SID and IAD.** [redacted] **percent of NTOC's budget execution authority for contracts and interagency acquisitions is executed outside the organization, resulting in insufficient oversight, of particular concern because of significant budget increases** [redacted]

(b) (1)
(b) (3)-P.L. 86-36

[redacted] expected for NTOC over the FY09-13 program.

(U) **Management Action All action officials have concurred with the recommendations, and Agency senior leadership has taken appropriate actions to resolve the disagreement about NTOC's mission.**

(U) Overall Report Classifications **TOP SECRET//COMINT//REL TO USA, FVEY**

(U) Category **Joint Warfighting and Readiness**

(U) **Hostile Work Environment and Reprisal**; NSA/CSS IG; IV-08-0023; 25 November 2008

(U//~~FOUO~~) **Summary** The OIG substantiated an allegation that a GG-14 managerial employee created a hostile work environment and subsequently reprised against a subordinate for reporting his inappropriate conduct to his supervisor. The investigation determined that the employee created a hostile work environment through inappropriate and intimidating conduct (swearing and throwing office items) and reprised against a subordinate who reported the misconduct.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Reprisal and Standards of Conduct)

(U) **Sexual Harassment and False Statement**; NSA/CSS IG; IV-08-0046; 14 January 2009

(U//~~FOUO~~) **Summary** The OIG substantiated an allegation that a GG-12 NSA supervisory police officer sexually harassed a junior police officer. The OIG determined that the senior officer made an unwelcome sexual advance toward the female junior officer. The investigation also determined that the officer knowingly and willfully made a false statement under oath during the investigation. A report was forwarded to the NSA Office of Employee Relations for a determination on disciplinary action.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Equal Employment Opportunity and Standards of Conduct)

(U) **Procurement Fraud Initiative**; NSA/CSS IG; Various Control Numbers; 1 October 2008 to 31 March 2009

(U//~~FOUO~~) **Summary** In October 2007, we launched an initiative to identify fraudulent billings by NSA contractors. This initiative involves data interrogation of contractor access records, coordination with contractor compliance officials, analysis of billing records, and investigation of access and billing anomalies.

(U//~~FOUO~~) Over the past six months, we have continued our initiative at NSA's Cryptologic Centers. As part of Phase II, we completed seven investigations at NSA/CSS Georgia and identified over 3,100 hours mischarged with an estimated recovery exceeding $200K. Some examples include:

(U//~~FOUO~~) **IV-09-0008** A contractor employee fraudulently billed the government 398 hours (approximately $42,000) over a 12 month period. The employee admitted to submitting false timesheets for late arrival and early departure each day.

(U//~~FOUO~~) **IV-09-0010** A contractor employee fraudulently billed the government

366 hours (approximately $21,000) over a 12 month period. The employee admitted to submitting false timesheets. Most of the discrepant hours represent excessive hours at lunch.

(U//~~FOUO~~) **IV-09-0019** A contractor employee fraudulently billed the government 249 hours (approximately $19,000) over a 12 month period. The employee admitted to submitting false timesheets. While the employee admitted leaving early, he was surprised that it was that much over a one year period.

(U//~~FOUO~~) During our analysis, we found potential mischarging by [redacted] contractors working at NSA/CSS Georgia and referred those to the [redacted] is conducting separate investigations. We believe these recoveries are significant. Additionally, we will commence a review of contractor program management during our contract labor reviews due to the significant amount of mischarging by contractor employees. Program management is one of the highest labor categories on most T&M contracts we have reviewed.

(U) **Category** Acquisition Processes and Contract Management

(b)(3)-P.L. 86-36

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U) **Advisory Report on Practices and Procedures To Ensure Accuracy of SIGINT Disseminated in Iraq and Afghanistan**; NSA/CSS IG; ST-08-0019; 17 December 2008

~~(S//REL)~~ **Summary Because Signals Intelligence (SIGINT) reportedly contributes to [redacted] in Iraq and Afghanistan, the Director of the SIGINT Directorate asked the NSA IG to examine current practices to ensure the accuracy and reliability of intelligence disseminated by SIGINT elements in-theater. Our advisory found [redacted]**

(U) **Management Action The recommendations in this advisory report are offered for the SIGINT Directorate leadership to consider after conducting a cost/benefit analysis of implementing the recommendations in a combat area.**

(U) Overall Report Classifications **SECRET//COMINT//REL TO USA, FVEY**

(U) Category **Joint Warfighting and Readiness**

(b)(1)
(b)(3)-P.L. 86-36

~~SECRET//REL TO USA, FVEY~~

UNITED STATES GOVERNMENT

memorandum

DATE: 01 April 2010 IG-11144-10

REPLY TO ATTN OF: Inspector General

SUBJECT: (U) Office of the Inspector General Semiannual Report to Congress-INFORMATION MEMORANDUM

TO: DIR _____
THRU: D/DIR _____

1. (U) The NSA/CSS Office of the Inspector General (OIG) submitted to the Inspector General, DoD, the attached Semiannual Report to the Congress on Intelligence-Related Oversight Activities for the period 01 October 2009 –31 March 2010.

2. (U//~~FOUO~~) This Report also satisfies a DoD requirement that Defense Intelligence Community Inspectors General provide a narrative input on their activities relating to counterterrorism (CT). I summarized the OIG's CT efforts in the last two pages of the Report.

3. (U//~~FOUO~~) If you require additional information, please contact [redacted], Deputy Inspector General, on 963-3544s.

(b) (3)-P.L. 86-36

George Ellard
Inspector General

cc: SID
IAD
CoS

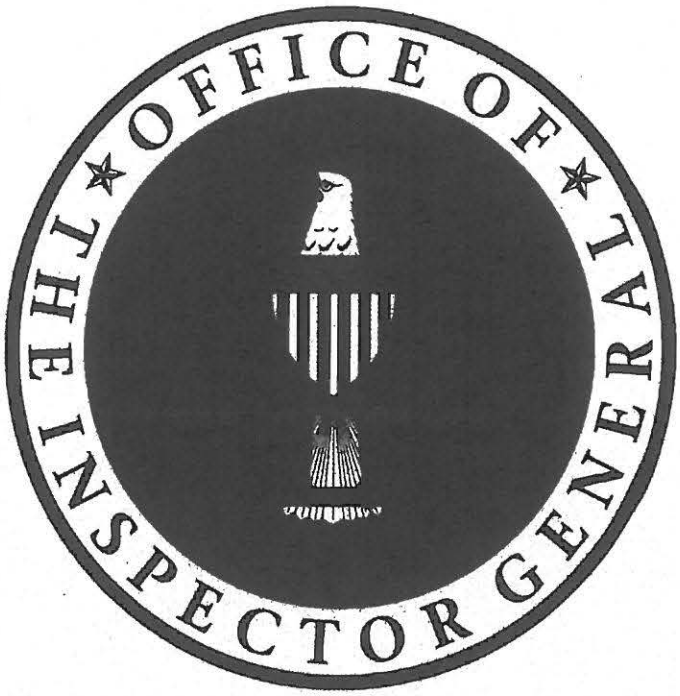
Encl:
a/s

This Document May Be Declassified Upon Removal of Enclosure and Marked UNCLASSIFIED//FOR OFFICIAL USE ONLY.

~~SECRET//REL TO USA, FVEY~~

~~SECRET//REL TO USA, FVEY~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE



INSPECTOR GENERAL REPORT

(U) SEMIANNUAL REPORT TO THE CONGRESS

October 01, 2009 – March 31, 2010

DERIVED FROM: NSA/CSSM 1-52
DATED: 20070108
DECLASSIFY ON: ~~20320108~~

(b) (3)-P.L. 86-36

(U) SEMIANNUAL REPORT TO THE CONGRESS

(U) ***For the Period October 1, 2009 through March 31, 2010***

(~~C//REL~~) **Intelligence Oversight of the Program at NSA/CSS Georgia;** NSA/CSS IG;

(~~C//REL~~) **Summary** During the investigation of alleged improprieties at NSA Georgia in 2004 and 2005 reported by a former assignee in 2008, the OIG identified some practices in that were inconsistent with established NSA/CSS policies and procedures. These practices included improper dissemination of raw SIGINT and noncompliance with quarterly reporting requirements. Our investigation also noted that Intelligence Oversight training was not uniform for all personnel performing the mission and did not adhere to the standards set in NSA/CSS policies.

(U//~~FOUO~~) **Management Action** Management concurred with our recommendations and is taking corrective action.

(U) **Overall Report Classification** SECRET//REL TO USA, FVEY

(U) **Category** Information Security and Privacy

(U) **Report on Congressional Budget Requests for the President's Surveillance Program;** NSA/CSS IG; ST-09-0018; 24 November 2009

(U//~~FOUO~~) **Summary** This is a compartmented study of how NSA reported to Congress on the President's Surveillance Program (PSP) in budget requests and budget briefings. On 17 June 2009, Counsel to the Senate Select Committee on Intelligence requested that the OIG review how the PSP had been reported in budget requests and briefings, given that only a few members of Congress had initially been aware of the program. This review responds to that request.

(U) **Overall Report Classification** TOP SECRET//COMINT//NOFORN (Compartmented)

(U) **Category** Information Security and Privacy

(U) **Management of Agency Firewalls**; NSA/CSS IG; AU-09-0002; 25 November 2009

(~~C//REL~~) **Summary** Firewalls are part of a defense-in-depth strategy used to protect Agency networks from cyber attack. The audit objective was to determine whether the Agency's firewalls are effective and efficient in securing the Agency's networks. The audit reviewed the Agency-wide policies and standards that govern the use of firewalls and how individual organizations manage and monitor them. Our audit found that the Agency

(U) **Management Action** The Technology Directorate concurred with our recommendations to improve the management of Agency firewalls.

(b) (1)
(b) (3)-P.L. 86-36

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(U) **Overall Report Classification** TOP SECRET//COMINT//NOFORN

(U) **Category** Information Security and Privacy

(U) **Annual Report to Congress on Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA)**; NSA/CSS IG; ST-10-0003; 30 November 2009

(~~S//REL TO USA, FVEY~~) **Summary** The Foreign Intelligence Surveillance Act Amendments Act of 2008 (FAA) authorizes the NSA/CSS OIG to assess the Agency's compliance with procedures for targeting certain persons outside the United States, other than United States persons. The OIG reviews the collection, processing, and reporting of data at least quarterly. Incidents involving compliance with procedures for targeting certain persons outside the United States, other than United States persons, and incidents involving minimization of United States person information are reported to the OIG as they occur and quarterly. Each incident is evaluated against the targeting and minimization procedures set forth in the FAA and in NSA directives. The report concluded that the OIG has no reason to believe that any intelligence activities of NSA during the period 1 September 2008 through 31 August 2009 were unlawful. In compliance with the targeting and minimization procedures of §702 of the FAA, the report included statistics on the total number of intelligence reports disseminated between FAA implementation on 1 September 2008 and 31 August 2009, including the total of those containing a reference to a United States person identity. The OIG also found and reported the total of instances of §702 targeting or minimization mistakes to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense for Intelligence Oversight.

(U//~~FOUO~~) **Management Action** Action was taken to correct the mistakes and processes were reviewed and adjusted to reduce the risk of unauthorized acquisition and improper retention of U.S. person communications.

(U) **Overall Report Classification** TOP SECRET//COMINT//REL TO USA, FVEY

(U) **Category** Information Security and Privacy

(b)(3)-P.L. 86-36

(U) [redacted] NSA/CSS IG; [redacted]

(~~S//REL TO USA, FVEY~~) **Summary** [redacted]

(U) **Management Action** The PMO is working to correct the deficiencies.

(U) **Overall Report Classification** TOP SECRET//COMINT//NOFORN

(U) **Category** Information Security and Privacy

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b) (3)-P.L. 86-36

(U) **Advisory Audit Report on Earned Value Management at NSA**; NSA/CSS IG; AU-09-0013; 12 February 2010

(U~~//FOUO~~) **Summary** Earned Value Management (EVM) is an important evaluation tool that alerts program managers to potential problems early in the program and reduces the chance and magnitude of cost overruns and schedule delays. Overall, our advisory audit found that NSA is complying with EVM policy; however, the use of EVM at NSA is limited. Only [redacted] contracts [redacted] use EVM. The Office of the Director National Intelligence and the Under Secretary of Defense for Acquisition, Technology and Logistics observed that many NSA contracts are level-of-effort (LOE), which is not structured to use EVM. To increase the use of EVM, NSA must change its contracting strategy of issuing LOE contracts, apply EVM to smaller dollar value contracts, and continue to develop a tailored EVM for government and contractor efforts.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Acquisition Processes and Contract Management

(U) **Annual Report to the Intelligence Oversight Board on NSA Activities – Calendar Year 2009**; NSA/CSS IG; ST-10-0008; 2 March 2010

(~~S//REL TO USA, FVEY~~) **Summary** Section 932 of the John Warner National Defense Authorization Act for FY 2007 (10USC 427) requires the Secretary of Defense to report to Congress annually on intelligence activities he has reason to believe may be unlawful or contrary to Executive Order or Presidential Directive. NSA's annual intelligence activities report, submitted to Congress via the Assistant to the Secretary of Defense for Intelligence Oversight, covered the 2009 activities that NSA reported to the Intelligence Oversight Board. Under the heading of Intelligence, Counterintelligence, and Intelligence-related activities that violate law, regulation, or policy substantiated during the year, as well as actions taken as a result of the violations, details were provided in the annual report for the following: 1) unintentional collection against U.S. persons or persons in the United States; 2) [redacted] and 3) an alleged unauthorized disclosure of classified information and misuse of the U.S. SIGINT System.

(U) **Overall Report Classification** TOP SECRET//COMINT//NOFORN

(U) **Category** Information Security and Privacy

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) **Yakima Research Station**; NSA/CSS IG; AFISRA IG; INSCOM IG; NNWC IG; JT-10-00001; 16 March 2010

(~~U//FOUO~~) **Summary** The IG organizations of the Air Force Intelligence, Surveillance, and Reconnaissance Agency, Naval Network Warfare Command, and NSA inspected the site in October 2009. Site leadership has overcome the number one challenge identified in the 2004 Joint Inspection of the Yakima Research Station, defining the site's role and engaging Higher Headquarters (HHQ) in solving problems. The widely disparate missions and associated challenges identified in this report have led to some confusion among the workforce about the strategic direction and mission priorities. Some problems identified in the previous IG report still exist and continue to reduce site effectiveness. Supporting programs (Intelligence Oversight, Training, Human Resources, Safety and Security) varied in their effectiveness. The training program showed general improvement, but still

requires additional attention for operations training and overall documentation of process and procedures. Intelligence Oversight at YRS is effective, but could be improved with additional direction and guidance from NSAW. The YRS HR programs provide a full range of services to the workforce. The lack of and inconsistent enforcement of some safety and security regulations have increased levels of risk in those areas.

(U) **Management Action** Management concurred with all recommendations and corrective actions are underway.

(U) **Overall Report Classification** SECRET//COMINT//REL TO USA, FVEY

(U) **Misuse of Government Resources**; NSA/CSS IG; IV-10-0008; CO-09-0806; 9 December 2009 and 29 January 2010.

(U~~//FOUO~~) **Summary** During routine monitoring of NSA/CSS unclassified computer systems, an NSA/CSS senior executive was detected accessing websites containing sexually-explicit images in violation of DoD regulation and Agency policy. During an OIG interview, the senior executive admitted to accessing the prohibited sites. The OIG referred a Report of Investigation (ROI) to the NSA/CSS Office of Employee Relations (ER). While ER was adjudicating the OIG's referral, the senior executive was once again detected accessing sexually-explicit websites, and once again admitted to accessing the websites during his OIG interview. The OIG referred a second ROI to ER for administrative discipline.

(U) **Management Action** The senior executive retired from the NSA/CSS prior to administration of discipline.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Standards of Conduct)

(U) **Misuse of Government Resources;** NSA/CSS IG; CO-09-0806, CO-09-0813, CO-10-0092, CO-10-0097, CO-10-0098, CO-10-0099, CO-10-0115, CO-10-0116, CO-10-0117, CO-10-0119, CO-10-0120, CO-10-0136, CO-10-0167, CO-10-0168, CO-10-0169, CO-10-0170, CO-10-0171, CO-10-0172, CO-10-0189, CO-10-0190, CO-10-0190, CO-10-0199. CO-10-0200, CO-10-0223, CO-10-0224, CO-10-0225, CO-10-0226, CO-10-0227, CO-10-0228, CO-10-0229, CO-10-0229, CO-10-0230, CO-10,0231, CO-10-0233, CO-10-0265, CO-10-0287, CO-10-0289, CO-10-0290, CO-10-0310, CO-10-0315, CO-10-0316, CO-10-0321, CO-10-0322, CO-10-0331, CO-10-0345, CO-10-0360, CO-10-0363, CO-10-0364, CO-10-0365, CO-10-0388, CO-10-0391; 1 October 2009 to 26 March 2010

(U~~//FOUO~~) **Summary** During the October 2009 to March 2010 time period, the OIG substantiated 50 allegations of misuse of government resources (e.g., accessing sexually-explicit material through the Agency's unclassified Internet network).

(U) **Management Action** Subjects in these cases were civilian employees, military affiliates, and NSA contractor employees. Discipline ranged from a letter of warning to reduction in grade.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Standards of Conduct)

(U) **Hostile Work Environment;** NSA/CSS IG; IV-10-0011; 25 February 2010.

(U~~//FOUO~~) **Summary** The OIG substantiated an allegation that a male Agency employee harassed and intimidated a female co-worker by using inappropriate language and engaging in unwanted physical contact with her.

(U) **Management Action** We referred our Report of Investigation to the NSA/CSS Office of Employee Relations for administrative discipline.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Sexual Harassment)

(U) **Time and Attendance Fraud**; NSA/CSS IG; IV-09-0022; 13 January 2010

(U~~//FOUO~~) **Summary** The OIG substantiated an allegation that an NSA/CSS civilian employee, a GG-15 Office Chief, knowingly submitted false time sheets from May 2008 to May 2009, for a total shortfall to the Government of 204.75 hours (approximately $12,600).

(U) **Management Action** We referred our Report of Investigation to the NSA/CSS Office of Employee Relations for administrative discipline.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Fraud

(U) **Time and Attendance Fraud** – NSA/CSS IG; IV-10-0007; 24 March 2010

(U~~//FOUO~~) **Summary** The OIG substantiated an allegation that an NSA/CSS civilian employee, a GG-7 Timekeeper, knowingly submitted false time sheets from June 2008 to October 2009, for a total shortfall to the Government of 291.75 hours (approximately $8,000).

(U) **Management Action** We referred our Report of Investigation to the NSA/CSS Office of Employee Relations for administrative discipline.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Fraud

(U) **Outside Employment**; NSA/CSS IG; IV-10-0005; 16 December 2009

(U~~//FOUO~~) **Summary.** The OIG substantiated an allegation that an Agency senior executive violated applicable DoD regulations and Agency policy by advertising and selling jewelry at work.

(U) **Management Action** We referred our Report of Investigation to the NSA/CSS Office of Employee Relations for administrative discipline.

(U) **Overall Report Classification** UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) **Category** Other (Standards of Conduct)

(U) **NSA OIG Anti-Fraud Initiative** – NSA/CSS IG; Various Control Numbers; Program Update

(U//~~FOUO~~) **Summary** In October 2007, we launched an initiative to identify fraudulent billings by NSA contractors. This initiative involved data interrogation of contractor access records, coordination with contractor compliance officials, and investigation of facility access and billing anomalies.

(U//~~FOUO~~) To date, we have completed over 100 labor mischarging investigations with approximately $2.2 million in recoveries. We are continuing to work in conjunction with the United States Attorney's Office in Baltimore and the Defense Criminal Investigative Service in regard to the criminal prosecution of the most egregious instances of fraud. Investigations completed over the past six months include the following:

(U//~~FOUO~~) **IV-09-0042** An NSA/CSS contractor affiliate billed the government 494 hours (approximately $56,600) over an 18-month period for unauthorized work. The company has offered to make restitution for the overbilling.

(U//~~FOUO~~) **IV-09-0045** An NSA/CSS contractor affiliate billed the government 380.75 hours (approximately $43,200) over a 12-month period for unauthorized work. The company has offered to make restitution for the overbilling.

(U//~~FOUO~~) **IV-09-0047** An NSA/CSS contractor affiliate billed the government 428.5 hours (approximately $41,000) over a 16-month period for unauthorized work. The company has offered to make restitution for the overbilling.

(U//~~FOUO~~) **IV-19-0054** An NSA/CSS contractor affiliate fraudulently billed the government 654 hours (approximately $34,000) over a 21-month period.

(U//~~FOUO~~) **IV-19-0055** An NSA/CSS contractor affiliate fraudulently over billed the government 121.5 hours (approximately $6,500) over a 21-month period.

(U//~~FOUO~~) **IV-19-0056** An NSA/CSS contractor affiliate fraudulently over billed the government 164 hours (approximately $15,900) over a 21-month period. The contractor affiliate also billed the government for 91.5 hours (approximately $8,500) of unauthorized work.

(U//~~FOUO~~) **IV-19-0057** An NSA/CSS contractor affiliate fraudulently over billed the government 98 hours (approximately $10,800) over a 21-month period.

(U//~~FOUO~~) **IV-19-0058** An NSA/CSS contractor affiliate fraudulently over billed the government 363.75 hours (approximately $20,000) over a 21-month period.

(U//~~FOUO~~) **IV-19-0059** An NSA/CSS contractor affiliate fraudulently over billed the government 190 hours (approximately $22,200) over a 21-month period. The contractor affiliate also billed the government for 37 hours (approximately $4,300) of unauthorized work.

(U//~~FOUO~~) **IV-19-0060** An NSA/CSS contractor affiliate fraudulently over billed the government 40.75 hours (approximately $3,800) over a 21-month period.

(U//~~FOUO~~) **IV-19-0061** An NSA/CSS contractor affiliate fraudulently over billed the government 678.75 hours (approximately $37,000) over a 21-month period.

(U//~~FOUO~~) **IV-19-0062** An NSA/CSS contractor affiliate fraudulently over billed the government 273.75 hours (approximately $26,000) over a 21-month period.

(U//~~FOUO~~) **IV-10-0010** An NSA/CSS contractor affiliate fraudulently over billed the government 366.75 hours (approximately $41,000) over an 11-month period.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) NSA/CSS OIG ACTIVITIES RELATED TO COUNTERTERRORISM

(U//~~FOUO~~) **Advisory Report on Second Follow-up Research on Expeditionary SIGINT Deployments to Hostile Areas**; NSA/CSS IG; ST-09-0008; 22 February 2010

(~~C~~//~~REL~~) **Summary** This is the second follow-up review of Hostile Area Deployment processes. Prior studies were completed in 2005 and 2007. Like the prior studies, this advisory review focused on [redacted]. We evaluated data culled from interviews and a web survey with NSA/CSS personnel who [redacted] In addition, we interviewed representatives of organizations involved in the deployment process. We found, since the last review in 2007, improvements in deployment processes continue, particularly in administrative processing, training, and medical and security processing, and [redacted] While progress has been noted, there is room for improvement in areas such as occupational health and environmental support services, and [redacted] processes. Periodic reviews of hostile area deployments are vital to ensure that NSA personnel are prepared to execute critical missions in support of Combatant Commands.

(U) **Overall Report Classification** CONFIDENTIAL//REL TO USA, FVEY

(U) **Category** Joint Warfighting and Readiness

(b)(3)-P.L. 86-36

Attached to this letter is the Semiannual Report to Congress by the Inspector General of the National Security Agency for the period 1 April to 30 September 2010.

I adopt the statistics and other information contained in that report.

Sincerely,

GEN Keith B. Alexander
USA

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20351001~~

~~SECRET//COMINT//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

Further dissemination of this report outside NSA is *PROHIBITED* without the approval of the Inspector General.

(U) SEMIANNUAL REPORT TO CONGRESS
1 April to 30 September 2010

George Ellard
Inspector General

Derived from: NSA/CSSM 1-52
Dated: 20101031
Declassify on: ~~20351031~~

(U) NSA OFFICE OF THE INSPECTOR GENERAL

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

(U) Intelligence Oversight

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

(U) Audits

(U) The OIG Office of Audits within the OIG provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) Investigations and Special Inquiries

(U) The OIG Office of Investigations administers a system for receiving and acting on requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips), at the request of management, as the result of questions that surface during inspections and audits, or at the initiative of the Inspector General.

(U) Field Inspections

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or by management request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with an assessment of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and other Intelligence Community Agencies to conduct joint inspections of consolidated cryptologic facilities.

~~SECRET//COMINT//NOFORN~~

(U) A MESSAGE FROM THE INSPECTOR GENERAL

(U) This report summarizes the more significant activities of the Office of the Inspector General (OIG) of the National Security Agency between 1 April and 30 September 2010. The report is mandated by the Intelligence Authorization Act of 2010.

(U) The most significant activity in the OIG during the reporting period was the continuing increase in the breadth and depth of the Office's expertise in information technology (IT), cyber, and intelligence oversight (IO). The NSA Director enabled this expansion of our capacities by supporting our efforts to hire superbly qualified recruits from the private sector and personnel steeped in NSA's mission from within the Agency.

(U) During the reporting period, the NSA OIG completed 60 audits, inspections, special studies, and investigations. The audits were almost evenly distributed across IO, IT, and mission programs.

(~~S//REL TO USA, FVEY~~) Completed IO reports included an advisory report on an OIG pilot test of NSA controls designed to ensure compliance with an Order of the Foreign Intelligence Surveillance Court (FISC) and monthly reports on OIG tests of FISC Order controls for January through July 2010. Reports related to mission programs included an audit of the Agency's Operational Test Authority, an audit of the Information Assurance Directorate's encryption interoperability, an audit of mission-assurance and continuity-of-operations compliance and testing, and a cyber research project. IT and cyber reports included an audit of [redacted] classified networks, an audit of the Agency's compliance with the Federal Information Security Management Act, and an audit of the Agency's Cross Domain Solutions.

(U) We also completed an external peer review of the investigative and audit offices within the OIG of the National Reconnaissance Office.

(U) The inspection staff completed reports on a joint inspection of the NSA/CSS Georgia Cryptologic Center and a headquarters inspection of the Agency's signals intelligence development strategy and governance.

(U) Special studies were completed on the [redacted] two SIGINT sites, data sharing with third-party partners, and the Selective Employment of Retirees/Standby Active Reserve Programs.

(U) The investigations staff opened 31 investigations and closed 44.

(b)(3)-P.L. 86-36

(U) Each report and special study contained recommendations on which the OIG and NSA management concurred, recommendations designed to improve the efficiency and effectiveness of the programs under review. The OIG tracks recommendations until they have been implemented and regularly reports to the NSA Director on the status of open recommendations. Of the 210 recommendations issued in the reporting period, 68 have been closed.

(b)(1)
(b)(3)-P.L. 86-36

George Ellard

George Ellard
Inspector General

~~SECRET//COMINT//NOFORN~~

DISTRIBUTION:

Dir
DDir
ExDir
CoS
D/C CSS
SID Dir
IAD Dir
CTO
RD
BMI
ODNI IG
DoD IG
CYBERCOM IG

cc:

LAO
OGC

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(U) INDEX OF REPORTING REQUIREMENTS

(U)

I.G. Act	Reporting Requirement	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	3-8
§5(a)(2)	Recommendations for corrective action	3-8
§5(a)(3)	Previously reported significant recommendations not yet completed	N/A
§5(a)(4)	Matters referred to prosecutive authorities	9
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	13
§5(a)(7)	Summary of significant reports	3-8
§5(a)(8)	Audit reports with questioned costs	17
§5(a)(9)	Audit reports with funds that could be put to better use	21
§5(a)(10)	Summary of reports for which no management decision was made	N/A
§5(a)(11)	Significant revised management decisions	N/A
§5(a)(12)	Management decision disagreements	N/A

(U)

(U) This page intentionally left blank.

(U) AUDITS OF PARTICULAR SIGNIFICANCE

(U) The Operational Test Authority

(U) The audit objective was to evaluate the effectiveness of the Agency's Operational Test Authority (OTA) as NSA's independent testing authority.

(U//~~FOUO~~) **Finding** The OTA is not independent because of its 2007 realignment under the Technology Directorate (TD), which is responsible for developing technology for major systems. TD can influence OTA because it controls OTA's budget and reviews OTA's suggested changes to Agency policies and guidance.

(U//~~FOUO~~) **Recommendation** The OIG recommended establishing an independent OTA with direct reporting authority to the NSA Director.

(b) (1)
(b) (3)-P.L. 86-36

(U) Cross Domain Solutions

(U//~~FOUO~~) The audit objective was to determine whether Cross Domain Solutions (CDSs) effectively and efficiently protect Agency networks. A CDS is a controlled interface that allows the secure transfer of data between domains with different security levels (e.g., Top Secret to Unclassified).

(~~S//NF~~) **Finding 1** Agency CDSs

(~~C//REL TO USA, FVEY~~) **Recommendation 1** The OIG recommended improving Agency CDS

(~~S//NF~~) **Finding 2** The Agency

(U//~~FOUO~~) **Recommendation 2** The OIG recommended developing a standard operating procedure (SOP) to document approved and allow system administrators to configure Agency CDSs. This SOP should require that changes be logged and controlled in an approved central repository.

(b) (3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U) Mission-Assurance Continuity-of-Operations Compliance and Testing

(U//~~FOUO~~) In August 2008, NSA identified 14 Mission Essential Functions (MEFs) that must be performed in all circumstances. As of August 2009, [redacted] Agency organizations had been identified as being responsible for performing essential tasks that support one or more of the 14 MEFs.

(~~C//REL TO USA, FVEY~~) **Finding** [redacted]

(~~U//FOUO~~) **Recommendation** The OIG recommended that the Agency track organization compliance in developing complete COOP plans and performing annual updates and testing.

(b)(1)
(b)(3)-P.L. 86-36

(U) INSPECTIONS OF PARTICULAR SIGNIFICANCE

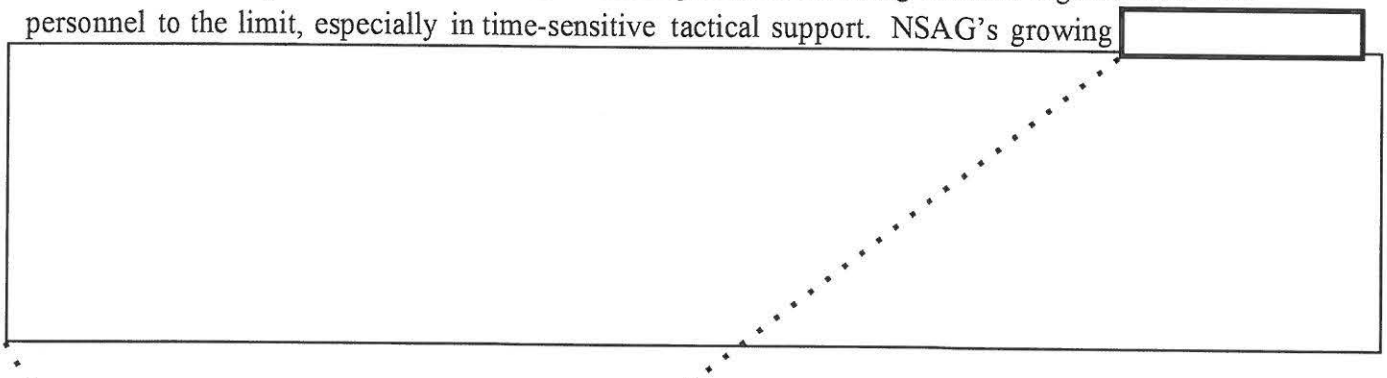
(U) NSA Georgia Cryptologic Center

(~~U//FOUO~~) During the reporting period the NSA Office of Inspections completed a Joint Inspection of the NSA Georgia (NSAG) Cryptologic Center at Fort Gordon, Georgia.

(U~~//FOUO~~) **Finding 1** Substantial growth in NSAG's Signals Intelligence, Information Assurance, and Computer Network Operations (CNO) missions and its information technology infrastructure has strained mission support resources. During the past five years, NSAG has experienced a large influx of joint and tactical personnel, who arrive without enabling support. They rely instead on NSA's heavily burdened support infrastructure. A root cause of this deficiency is the lack of clear manpower and budget requirements necessary to operate the cryptologic center.

(~~U//FOUO~~) **Recommendation 1** NSA Headquarters and NSAG should define, program for, and provide the minimum mission enabler personnel and funds needed to operate the Center effectively.

(~~C//REL TO USA, FVEY~~) **Finding 2** There are not enough joint operations personnel at NSAG to meet tactical mission requirements. Continued mission growth is stressing mission organizations and personnel to the limit, especially in time-sensitive tactical support. NSAG's growing



(~~U//FOUO~~) **Recommendation 2** The NSA Signals Intelligence Director should develop a business plan for the prioritization and appropriate distribution of tactical missions and associated resources at NSAG, taking into consideration the demands that additional mission will put on the site.

(b)(1)
(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) SPECIAL STUDIES OF PARTICULAR SIGNIFICANCE

(b) (1)
(b) (3)-P.L. 86-36

(U) Data Sharing with Third-Party Partners

(~~S//REL TO USA, FVEY~~) NSA's third-party partners are nations other than Australia, Canada, New Zealand, and the United Kingdom with which the U.S. government has national Signals Intelligence (SIGINT) arrangements. The purpose of the review was to determine whether policies and procedures are in place to ensure compliance with authorities for sharing [redacted] with third-party partners. [redacted]

(~~S//NF~~) **Finding 1** Updated policies and process improvements are needed. Documentation for [redacted] disseminated to third-party partners is not centrally maintained. Limited documentation is scattered across many locations throughout the SIGINT Directorate (SID) and the Foreign Affairs Directorate (FAD). Documentation in FAD's Foreign Affairs Knowledge System is not current or easily retrievable.

(~~S//REL TO USA, FVEY~~) **Recommendation 1** FAD should establish a repository for documenting [redacted] shared with third-party partners, and it should update existing documentation.

(~~S//REL TO USA, FVEY~~) **Finding 2** Although SID's Analysis and Production Directorate (S2) developed a process in February 2007 to [redacted] disseminated to third-party partners, the process is not well understood, and it has never been reviewed. Quarterly guidance to the S2 workforce on how to [redacted] disseminated to partners is unclear, and, as a result, [redacted] is inconsistent.

(~~S//SI//REL TO USA, FVEY~~) **Recommendation 2** SID should revise its oversight process for disseminating [redacted] to partners, including [redacted] procedures, and inform the workforce of the revised process. SID should also publish an approval authority matrix for third-party activity and formal training on third-party partnerships and provide it to NSA personnel.

(~~S//SI//REL TO USA, FVEY~~) **Finding 3** SID lacks a standard process for [redacted]

(~~S//REL TO USA, FVEY~~) **Recommendation 3** SID should establish a standard process [redacted]

(b) (1)
(b) (3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~) The

(U//~~FOUO~~) After the 11 September 2001 terrorist attacks on the United States, NSA established a Since then, has undergone several reorganizations; most recently, became an element of the SIGINT Development Strategy and Governance organization.

(U//~~FOUO~~) **Finding 1** lacks essential mission documentation and standards for NSA Headquarters and the Extended Enterprise.

(~~C//REL TO USA, FVEY~~) **Recommendation 1** should develop a Mission and Functions Statement, Strategic Plan, and implementing instructions, reflecting the evolving mission of external agencies. The documents should clearly define internal management controls in standard operating procedures, system configuration management, and budget documentation.

(U//~~FOUO~~) **Finding 2** has no Intelligence Oversight program.

(U//~~FOUO~~) **Recommendation 2** The should establish an Intelligence Oversight program in accordance with Department of Defense regulations and NSA policies.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) INVESTIGATIONS OF PARTICULAR SIGNIFICANCE

(U) Summary of Prosecutions

(U) Indictment

(U) An Agency employee was indicted in June 2010 for accepting more than $110,000 in bribes from a contractor as part of a scheme to defraud NSA. The trial is scheduled for January 2011 in the United States District Court in Baltimore, MD.

(U) Conviction

(U) A former Agency contractor pled guilty in July 2010 to submitting false labor charges for approximately $82,000. Sentencing occurred in October 2010 in the United States District Court in Baltimore, MD.

(U) Referrals

- (U) An Agency employee and timekeeper submitted 531.75 hours of false labor charges for a loss to the government of approximately $22,000. The case was presented to the Office of the United States Attorney for the District of Maryland in August 2010 and was accepted for prosecution.
- (U) A former Agency subcontractor submitted 34 false travel vouchers from 2007 to 2009 with claims of approximately $21,000. In May 2010, the case was presented to the Office of the United States Attorney for the District of Maryland. A decision on prosecution is pending.
- (U) An Agency contractor violated 18 U.S.C. §208 because he returned to NSA as a contractor within one year of his retirement as an NSA senior employee. The Office of the United States Attorney for the District of Maryland declined prosecution in July 2010.
- (U) Nine cases of contractor labor mischarging were referred to the Office of the United States Attorney for the District of Hawaii. Five cases have been declined for prosecution; decisions are pending on four. The amount of possible labor mischarging in these cases is approximately $180,000.
- (U) Ten cases of contractor labor mischarging were referred to the Office of the United States Attorney for the District of Maryland and were declined for prosecution. The possible mischarging in these cases was approximately $424,000.

(U) This page intentionally left blank.

(U) APPENDIX A

(U) AUDITS, INSPECTIONS, AND SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD

This page intentionally left blank.

(U) APPENDIX A

(U) AUDITS, INSPECTIONS, AND SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD

(U) Audits

- (U) The Cryptographic Interoperability Strategy/Suite B
- (U) Mission-Assurance Continuity-of-Operations Compliance and Testing
- (U) Compliance with the Federal Information Security Management Act
- (U) The Operational Test Authority
- (~~S//REL TO USA, FVEY~~) Cyber Security: NSA Response to [redacted] Classified Networks
- (U) Cross Domain Solutions
- (U) External Peer Review of NRO

(b)(1)
(b)(3)-P.L. 86-36

(U) Inspections

- (U//~~FOUO~~) SIGINT Development Strategy and Governance
- (U) NSA Georgia Cryptologic Center

(U) Special Studies

- (U//~~FOUO~~) NSA Controls for a Classified Program (and monthly test reports from March through August 2010)
- (U//~~FOUO~~) [redacted]
- (U) Selective Employment of Retirees and Standby Active Reserve Programs
- (U) [redacted]
- (U) Cyber Research
- (U) Data Sharing with Third-Party Partners

(b)(3)-P.L. 86-36

(U) This page intentionally left blank.

(U) APPENDIX B

(U) AUDIT REPORTS WITH QUESTIONED COSTS

(U) This page intentionally left blank.

(U) APPENDIX B

(U) AUDIT REPORTS WITH QUESTIONED COSTS

(U)

Report	Number	Questioned Costs	Unsupported Costs
For which no management decision had been made by start of reporting period	0	0	0
Issued during reporting period	0	0	0
For which management decision was made during reporting period	0	0	0
Costs disallowed	0	0	0
Costs not disallowed	0	0	0
For which no management decision was made by end of reporting period	0	0	0

(U)

(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.

(U) This page intentionally left blank.

(U) APPENDIX C

(U) AUDIT REPORTS OF FUNDS THAT COULD BE PUT TO BETTER USE

(U) This page intentionally left blank.

(U) APPENDIX C

(U) AUDIT REPORTS OF FUNDS THAT COULD BE PUT TO BETTER USE

(U)

Report	Number	Amount
For which no management decision had been made by start of reporting period	0	0
Issued during reporting period	0	0
For which management decision was made during reporting period	0	0
Value of recommendations agreed to by management	0	0
Value of recommendations not agreed to by management	0	0
For which no management decision was made by end of reporting period	0	0

(U)

(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

(U) SEMI-ANNUAL REPORT TO CONGRESS
1 October 2010 to 31 March 2011

Derived from: NSA CSSM 1-52
Dated: 20070108
Declassify on: ~~20320108~~

(U) NSA OFFICE OF THE INSPECTOR GENERAL

(U) The NSA Office of the Inspector General (OIG) conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources, and ensure that NSA activities are conducted in compliance with the law. The OIG also serves as an ombudsman, assisting Agency employees, civilian and military, with complaints and questions.

(U) Intelligence Oversight

(U) The OIG Office of Intelligence Oversight reviews NSA's most sensitive and high-risk programs for compliance with the law.

(U) Audits

(U) The OIG Office of Audits provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and assess whether NSA operations comply with federal policies. Information Technology audits determine whether IT solutions meet customer requirements, while conforming to information assurance standards. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) Investigations and Special Inquiries

(U) The OIG Office of Investigations administers a system for receiving and acting on requests for assistance and complaints about fraud, waste, and mismanagement. Investigations and special inquiries may be undertaken as a result of such requests and complaints (including anonymous tips), at the request of management, as the result of questions that surface during inspections and audits, or at the initiative of the Inspector General.

(U) Field Inspections

(U) The Office of Field Inspections conducts site reviews as part of the OIG's annual plan or at management's request. Inspections yield accurate, up-to-date information on the effectiveness and efficiency of field operations and support programs, along with assessments of compliance with federal policy. The Office partners with Inspectors General of Service Cryptologic Components and other Intelligence Community agencies to conduct joint inspections of consolidated cryptologic facilities.

(U) A MESSAGE FROM THE INSPECTOR GENERAL

(U) This report summarizes the more significant activities of the Office of the Inspector General (OIG) of the National Security Agency between 1 October 2010 and 31 March 2011. The report is mandated by the Intelligence Authorization Act of 2010.

(U) During the reporting period, the NSA OIG completed 28 audits, inspections, special studies, and investigations.

(U) The Audits Division completed nine audits ranging from federal compliance to Information Technology to financial management and operations. The OIG rarely issues reports without a management decision and on only a few occasions does the OIG encounter non-concurrence with its recommendations. In this reporting period, however, the Audit Report of NSA/CSS Enterprise Solution and Baseline Exception Request Processes contained one non-concurrence. The Director has resolved this situation.

(U) The Inspections Division completed reports on a field inspection of Cryptologic Services Group –Marine Corps Intelligence Agency and joint inspections of Menwith Hill Station and NSA activities at the U.S. Central Command.

(U//~~FOUO~~) The OIG completed special studies on SIGINT Support [redacted] and Foreign Intelligence Surveillance Court Rule 13(a) and 13(b) filings.

(U) The Investigations Division fielded 477 contacts from the OIG Hotline. The team opened 20 investigations and closed 11 in the reporting period.

(U) Each report and special study contained recommendations on which the OIG and NSA management concurred, recommendations designed to improve the efficiency and effectiveness of the programs under review. The OIG tracks recommendations until they have been implemented and regularly reports to the NSA Director on the status of open recommendations. Of the 274 recommendations issued in the reporting period, 70 have been closed.

(b)(3)-P.L. 86-36

George Ellard
Inspector General

(U) DISTRIBUTION:

DIR
DDIR
ExDIR
CoS
SID Dir
IAD Dir
TD Dir
LAO
OGC
ODOC
FAD
BMI
SAE
ODNI IG
DoD IG

(U) TABLE OF CONTENTS

(U) This page intentionally left blank.

(b)(1)
(b)(3)-P.L. 86-36

(U) AUDITS

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(U) Completed Audits

(U//~~FOUO~~) **Audit of Data Sharing with Third-Party Partners** (20 September 2010) (published in previous quarter but not listed in the quarterly report, which was submitted early)

(~~TS//SI//NF~~) In 2009, NSA sent more than [redacted] messages to Third Party partners [redacted] Completion of recommended actions will reduce the risk associated with disseminating [redacted] to Third Parties.

(U) **Audit of Educational Assistance and Recruitment Programs** (18 November 2010)

(U//~~FOUO~~) NSA/CSS spends approximately [redacted] a year on incenti ves to meet its skill needs, including scholarship awards to students majoring in critical fields, tuition assistance to employees taking college courses, bonus compensation to employees relocating to field sites, and recruitment bonuses to employees who staff hard-to-fill positions. The audit found that standard processes for overseeing scholarship programs are lacking. The Agency has initiated action to recoup approximately $1 million in tuition payments from employees whose grades did not meet eligibility requirements for tuition assistance.

(b)(3)-P.L. 86-36

(U) **Audit of the FISA Amendments Act §702 Detasking Requirements** (24 November 2010)

(~~S//REL TO USA, FVEY~~) Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 (FAA) has strengthened SIGINT collection, particularly against terrorist targets. From September 2008 to March 2010, the number of SIGINT reports that incorporated FAA §702 sourced collection grew from fewer than [redacted] to more than [redacted] and the percentage of counterterrorism reporting with a contribution from FAA §702 collection rose steadily from [redacted] to [redacted] percent.

(~~TS//SI//NF~~) However, collection under FAA §702 must cease under certain circumstances to remain lawful, potentially resulting in gaps in coverage. To regain coverage, NSA must transition to another authority, [redacted] for continued collection. [redacted]

(U//~~FOUO~~) **Audit of the Nuclear Weapons Personnel Reliability Program** (28 December 2010)

(U//~~FOUO~~) The purpose of the Nuclear Weapons Personnel Reliability Program (NWPRP) is to ensure that all NSA/CSS personnel who perform nuclear weapons-related duties meet the highest standards of reliability, including physical, psychological, and technical competence. The audit concluded that NWPRP provides reasonable assurance that only the most reliable individuals perform duties associated with nuclear weapons. The audit did identify a problem in drug-testing methodology. Agency managers agreed to fix the problem.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(~~TS//SI//NF~~) **Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – December 2010** (monthly test reports from August through December 2010)

(~~TS//SI//NF~~) This report summarizes results of tests of controls for December to ensure NSA's compliance with seven requirements of the Foreign Intelligence Surveillance Court Order Regarding Business Records (BR). The monthly tests were conducted throughout 2010 as part of the continuous auditing methodology and to meet OIG oversight requirements of the BR Order. The report found that NSA controls over querying were adequate to provide reasonable assurance of compliance with the five provisions of the Order that were tested. The report also found that although manual controls over the dissemination of serialized Signals Intelligence reports and the compilation of the Weekly Dissemination Reports are inherently risky, they are acceptable given the amount of information disseminated [ ] reports during 2010).

(U) **Audit of Firewall Management for CES and** [ ] (28 January 2011)

(~~C//REL TO USA, FVEY~~) We reviewed [ ] organizations that operate and maintain firewalls that protect the Cryptanalysis and Exploitation Service (CES) and [ ] and found [ ]

Technology Directorate and Signals Intelligence Directorate have concurred with our recommendations to improve the management of CES and [ ] firewalls.

(b) (3)-P.L. 86-36

(U) **Audit of Market Research and Competition** (31 January 2011)

(U//~~FOUO~~) Market research and competition are essential to fair pricing. The objective of this audit was to determine whether the Agency is adequately seeking competition in contracting and whether adequate market research is being conducted and documented. The audit found that the Acquisition Resource Center is an effective tool, but staffing levels need review; competition statistics are inaccurate because of coding errors; definition of competition needs revision; and market research documentation needs improvement. Management is addressing the recommendations.

(U) **Oversight Review of the Restaurant Fund, Civilian Welfare Fund, and Cryptologic Museum Gift Shop** (18 March 2011)

(U) This report summarizes the results of our oversight review of the audit of the Restaurant Fund (RF), the Civilian Welfare Fund (CWF), and the Cryptologic Museum Gift Shop for FY2010 by a Certified Public Accountant firm. The objective was to ensure that the audit of the RF, CWF, and Cryptologic Museum Shop was consistent with Government Auditing Standards. We concluded that it was, and the CPA firm did not identify management concerns.

(U) **Audit of the Power, Space, and Cooling Triage Process for the Extended Enterprise** (25 March 2011)

(U//~~FOUO~~) The Power, Space, and Cooling Triage process is operating as intended. The [ ] extended enterprise sites that participate in the process have improved management of their power requirements. However, one significant problem is the inability of participating sites to measure power usage consistently because of a lack of standardized capability to monitor power.

(U) **Audit of NSA/CSS Enterprise Solution and Baseline Exception Request Processes** (31 March 2011)

(U//~~FOUO~~) The Technology Directorate established the National Security Agency/Central Security Service Enterprise Solution (NES) and Baseline Exception Request (BER) processes to reduce Information Technology (IT) complexity, improve interoperability and security, and manage IT costs. Our review found that Agency organizations and contractors [redacted] Without functioning controls to ensure compliance, the Agency and its Chief Information Officer (CIO) will be unable to manage effectively IT items purchased and installed by Agency organizations and its contractors. Management concurred with all but one recommendation.

(U) Audits of Particular Significance

(U) **Audit Report of NSA/CSS Enterprise Solution and Baseline Exception Request Processes** (31 March 2011)

(U) **QUESTIONED COSTS**

(b)(3)-P.L. 86-36

(U//~~FOUO~~) This audit uncovered [redacted] worth of IT purchases that Agency organizations and contractors acquired under a fictitious BER approval number. Management will review a representative sample of these requisitions to determine whether the questioned costs were in compliance with the NES Baseline and take the appropriate action if the item purchased was not compliant. If the sample shows significant rates of non-compliance, the review will be extended to all requisitions under the fictitious number. In the meantime, new control processes have been implemented to prohibit future use of fictitious approval numbers. The processes involve Enterprise Information Technology, Directorate of Resources Management, and Directorate of Acquisition. This review will also provide insight on how to strengthen the controls being designed in response to other OIG recommendations made in this report.

(U) Significant Recommendations Outstanding in Previous Semi-annual Reports

(U) **Audit of Operational Test Authority** (12 May 2010)

(U) The audit objective was to evaluate the effectiveness of the Agency's Operational Test Authority (OTA) as NSA's independent testing authority.

(U//~~FOUO~~) **Finding** The OTA is not independent because of its 2007 realignment under the Technology Directorate (TD), which is responsible for developing technology for major systems. TD can influence OTA because it controls OTA's budget and reviews OTA's suggested changes to Agency policies and guidance.

(U//~~FOUO~~) **Recommendation 1** The OIG recommended establishing an independent OTA with direct reporting authority to the NSA Director. **UPDATE:** This recommendation is now CLOSED.

(U) **Audit of Cross Domain Solutions** (23 June 2010)

(U//~~FOUO~~) The audit objective was to determine whether Cross Domain Solutions (CDSs) effectively and efficiently protect Agency networks. A CDS is a controlled interface that allows the secure transfer of data between domains with different security levels (e.g., Top Secret to Unclassified).

(~~S//REL TO USA, FVEY~~) **Finding** Agency CDSs [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) **Recommendation 1** The OIG recommended improving [redacted] Agency CDS [redacted] for all operational CDSs.

(~~S//NF~~) **Finding** The Agency [redacted]

(U//~~FOUO~~) **Recommendation 5** The OIG recommended developing a standard operating procedure (SOP) to document approved [redacted] This SOP should require that changes be logged and controlled in an approved central repository. **UPDATE:** This recommendation is now CLOSED.

(b) (3)-P.L. 86-36

(U) **Audit of Mission-Assurance Continuity of Operations Compliance and Testing** (17 August 2010)

(U//~~FOUO~~) In August 2008, NSA identified 14 Mission Essential Functions (MEFs) that must be performed in all circumstances. As of August 2009, [redacted] Agency organizations had been identified as being responsible for performing essential tasks that support one or more of the 14 MEFs.

(~~C//REL TO USA, FVEY~~) **Finding** [redacted]

(U//~~FOUO~~) **Recommendation 1** The OIG recommended that the Agency track organization compliance in developing complete COOP plans and performing annual updates and testing.

(U) Ongoing Audits

(U) **Audit of NSA Police Operations**

(U//~~FOUO~~) The audit objective is to evaluate the effectiveness and efficiency of the National Security Agency Police (NSAP) at NSA/CSS Washington (NSAW), specifically to determine whether NSAP is adequately equipped, staffed, and trained to protect and defend NSAW personnel and property.

(U) **Audit of Agency Controls for [redacted] IT Hardware Purchases**

(U//~~FOUO~~) The audit objective is to determine whether the Agency's internal controls effectively reduce the risk for [redacted] Technology purchases.

(U) **Audit of NSA/CSS's Wireless Networks and Devices**

(U) The audit objective is to assess Agency controls for protecting against unauthorized operation of wireless networks and devices within NSA/CSS spaces and to assess Agency wireless implementation initiatives.

(U) **Audit of High-Performance Computing**

(U) The audit objective is to evaluate the contracting process of the High Performance Computing – Special Program Office.

(U) **Audit of Information Sharing**

(U) The audit objective is to review Agency effectiveness in sharing cyber threat and vulnerability information with other Intelligence Community agencies in accordance with the Comprehensive National Cyber Initiative.

(U) **Audit of the Acquisition Security Process**

(U) The audit objective is to determine whether the Acquisition Security process effectively and efficiently mitigates the foreign ownership, control, or influence and counterintelligence risk of the Agency's information technology purchases.

(U) **Audit of the ARCANAPUP Modernization Effort**

(U) The audit objective is to determine the effectiveness of ARCANAPUP in meeting program goals.

(U) **Audit of Nuclear Command and Control (NC2) Program**

(U) The audit objective is to determine whether NSA implemented corrective actions to satisfy recommendations made in previous audits and reviews of the NC2 process.

(U) **Audit of NSA's Compliance with National Security Directive 42 to Support Non-DoD Agencies for Network Intrusions**

(U) The audit objective is to determine whether the Information Assurance Directorate is effectively fulfilling the Agency's responsibilities for network intrusion support to non-DoD agencies in accordance with National Security Directive 42, *National Policy for the Security of National Security Telecommunication and Information Systems*, 5 July 1990.

(U) **Audit of General Application Controls for Agency Payroll, Human Resources, and Contracting Systems**

(U) The audit objective is to assess the general and application controls of the Agency's payroll, human resources, and contractor systems. Specifically, the NSA Comptroller has requested that we review the Defense Civilian Payroll System, the Human Resources Management System, and the Contracting Management Information System.

(U) This page intentionally left blank.

(U) INSPECTIONS

(U) Completed Inspections

(U) **Joint Inspection of Alaska Mission Operations Center** (8 October 2010)

(U//~~FOUO~~) The Alaska Mission Operations Center (AMOC) has made significant progress since its first Joint IG inspection in 2006. Site leadership is actively engaged in mission and working diligently to shift the culture from an Air Force-focused site to an NSA/CSS site. Site leadership is trying to balance mission needs and resources based on inadequate guidance and documentation from NSA/CSS. The site uses mission personnel to supplement necessary enabling functions resulting from increased mission growth and an increase in NSA/CSS civilian personnel. An appropriate skill mix is hard to determine because much of the mission is not formally documented. [redacted] The future for AMOC includes new mission sets, more customer engagement, and aggressive partnership development, all of which could place additional burdens on an already stretched workforce.

(U) **Field Inspection of Cryptologic Services Group–Marine Corps Intelligence Agency** (1 December 2010)

(U//~~FOUO~~) The field inspection of the Cryptologic Services Group (CSG)–Marine Corps Intelligence Agency (MCIA) found a number of serious problems with the organization's readiness to accomplish its assigned mission. Although manning numbers are sufficient, the majority of personnel [redacted] CSG training, intelligence oversight, and mission guidance to junior personnel were not sufficient. We also found that [redacted] Recommendations have been formally tasked for action.

(b)(3)-P.L. 86-36

(U) **Joint Inspection of Menwith Hill Station** (14 December 2010)

(~~C//REL TO USA, FVEY~~) Mission accomplishment at Menwith Hill Station is successful. However, [redacted] NSA/CSS and other agency mission sponsors must provide guidance to the site on mission prioritization. The lack of agreement on cost-sharing Memoranda of Understanding and [redacted] remains of significant concern; however, significant progress has been made toward resolving both findings since the inspection. Continued [redacted] and repeated delays in military construction funding for family housing projects affect quality of life for assigned personnel. Recommendations have been formally tasked for action.

(b)(1)
(b)(3)-P.L. 86-36

(U) **Joint Inspection of NSA Activities at U.S. Central Command** (4 March 2011)

(U//~~FOUO~~) Leadership has built a positive, mission-oriented workforce. In almost every area, however, inspectors found processes that were successful yet undocumented. Lack of formal guidance makes it difficult at times for NSA/CSS Representative to Central Command (NCRCENT) personnel to support NSA interests effectively. Implementation of field governance is applied inconsistently across the [redacted] Furthermore, NSA Headquarters' over-reliance on Staff Processing Forms makes it difficult to operate in a fast-paced operational environment. [redacted] Lack of promotion opportunities, as a result of civilian promotion caps, [redacted] Recommendations have been formally tasked for action.

(U) Inspections of Particular Significance

(U) **Joint Inspection of Menwith Hill Station** (14 December 2010)

(b)(3)-P.L. 86-36

(U) **REFERRAL: Problems with DoDEA School Administration**

(U//~~FOUO~~) Although not within the scope of an Intelligence Community inspection, the Menwith Hill Station (MHS) Joint Inspection Team identified, documented, and addressed widespread, longstanding discontent with perceived lack of professionalism by the on-base Department of Defense Education Activity (DoDEA) School administrators and teachers. The situation adversely affects the station's quality of life and mission operations. A Joint Inspector General (IG) town hall meeting was conducted to gain a better understanding of the scope of school-related issues. The meeting was attended by approximately [redacted] parents, many of whom were extremely frustrated by their inability to resolve issues despite numerous visits and telephone calls to the school. The IG's concern about degradation of mission operations and MHS quality of life drove our decision to include this in our report. The 2007 MHS Joint IG Inspection also documented concerns with effective administration, management, and discipline in the MHS DoDEA School. The Joint Inspection Team findings were formally referred to the DoD IG as a matter under its purview. Updates from the site indicate that the referral resulted in increased scrutiny from the DoDEA regional administration and that the local school administration has begun to make positive changes.

(U) Significant Recommendations Outstanding in Previous Semi-annual Reports

(U) **Joint Inspection of** [redacted] (17 November 2008)

(U) **FINDING: Fire Suppression System Lacking**

(U//~~FOUO~~) Lack of a fire suppression system in [redacted] seriously degrades the ability to protect life and critical equipment. This deficiency was initially identified during a 1997 Joint Inspector General inspection and was again noted in an NSA Occupational Health and Environmental Survey conducted in 2000. Overall stewardship of [redacted] facilities is the responsibility of [redacted] Planning for fire suppression system installation began in May 2001; however, no stakeholder agencies committed the needed funding. Although it remained a critical safety deficiency, no further progress was made until September 2009, when the Director, NSA emphasized the need to complete the action. [redacted] contracted for system

design, followed by a phased installation in 2010 using consolidated cryptologic program funding. The installation is now 37% complete. A projected completion date of November 2011 remains tentative because of [redacted] and possible delays in getting supplies needed to complete the installation.

(U) **Multiple Joint Inspections from FY2005 to FY2010 Regarding USSID CR1200**

(~~C//REL TO USA, FVEY~~) *Concept of SIGINT Support to Military Commanders* provides policy and guidance on Signals Intelligence (SIGINT) support to military commanders and operations. Published in 1998, this United States Signals Intelligence Directive (USSID) is severely outdated, contains obsolete functions and terminology not used in current military doctrine, provides no Higher Headquarters template for present-day Military Operations Integration, and does not establish standards for expeditionary SIGINT support for ongoing military operations. This significant deficiency was noted as a finding in inspection reports encompassing [redacted] Global Cryptologic Enterprise Sites beginning in FY2005 (Reference Findings: [redacted] and continuing to the present. An NSA/CSS action element is leading a working group with stakeholder participation to draft a new USSID as recommended in this inspection report. The action element determined that other supporting policy documents must first be updated; there is no estimated completion date for this critical document.

(U) **Joint Inspection of NSA/CSS Georgia** (30 June 2010)

(U//~~FOUO~~) **Finding** Substantial growth in NSA/CSS Georgia's (NSAG) Signals Intelligence, Information Assurance, and Computer Network Operations (CNO) missions and its information technology infrastructure has strained mission support resources. During the past five years, NSAG has experienced a large influx of joint and tactical personnel, who arrive without enabling support. They rely instead on NSA's heavily burdened support infrastructure. A root cause of this deficiency is the lack of clear manpower and budget requirements necessary to operate the cryptologic center.

(U//~~FOUO~~) **Recommendation FG-10-2036** NSA Headquarters and NSAG should define, program for, and provide the minimum mission enabler personnel and funds needed to operate the Center effectively. **UPDATE:** This recommendation is now CLOSED.

(~~C//REL TO USA, FVEY~~) **Finding** There are not enough joint operations personnel at NSAG to meet tactical mission requirements. Continued mission growth is stressing mission organizations and personnel to the limit, especially in time-sensitive tactical support. NSAG's growing [redacted]

(U//~~FOUO~~) **Recommendation FG-10-2001** The NSA Signals Intelligence Director should develop a business plan for the prioritization and appropriate distribution of tactical missions and associated resources at NSAG, taking into consideration the demands that additional mission will put on the site. **UPDATE**: This recommendation is now CLOSED.

(U) Ongoing Inspections

(U) **Joint Inspection of NSA/CSS Hawaii**

(U//~~FOUO~~) The NSA/CSS Office of Inspections conducted a Joint Inspection of NSA/CSS Hawaii between 24 January and 4 February 2011. The final report is in coordination.

(U) **Expeditionary Operations Review of** [redacted]

(U//~~FOUO~~) The Inspections Team conducted a review of NSA activities [redacted] from [redacted] The draft report is in coordination.

(b)(3)-P.L. 86-36

(U) SPECIAL STUDIES

(b) (3)-P.L. 86-36

(U) Completed Special Studies

(U) **Special Study of SIGINT Support to** (10 February 2011)

~~(TS//SI//NF)~~ The objective of this special study was to assess procedures and controls used to provide Signals Intelligence (SIGINT) support The study focused on support to We reviewed mission management, analytic techniques, and SIGINT dissemination. With few exceptions, NSA/CSS support was effective, and SIGINT reporting complied with Agency directives. However, NSA/CSS has not established a common definition, qualification or proficiency standards, or formal training for operational support policy should be improved, CT operational security should be reviewed, and the role of the CT Mission Management Center should be clearly delineated; and reporting guidance is ambiguous, does not effectively address and has inconsistent reporting standards. The corrective actions planned by management meet the intent of the recommendations.

(U//~~FOUO~~) **Review of Foreign Intelligence Surveillance Court (FISC) Rule 13(a) and 13(b) Filings** (22 March 2011)

(U//~~FOUO~~) FISC Rule 13(a) requires the government to immediately correct misstatements or omissions of material facts in submissions to the FISC. Rule 13(b) requires the government to immediately inform the FISC of incidents outside the scope of the Court's authorization. The NSA Office of General Counsel (OGC) coordinates the filing of notices with the US Department of Justice, the final author of 13(a) and 13(b) notices. The OIG reviewed 13(a) and 13(b) filings from September 2009 through November 2010 for timeliness and accuracy. In that period, no FISC notices were amended because of material misstatements within the initial FISC incident reports. However, we observed that OGC does not maintain a central repository or tracking system for 13(a) and 13(b) filings. During our review, the Signals Intelligence Directorate and OGC adopted a process to address timeliness concerns. We will consider conducting another review when that process matures.

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(U) Special Studies of Particular Significance

(U) **Special Study of SIGINT Support to** 10 February 2011)

~~(TS//SI//NF)~~ NSA/CSS in support of counter-terrorism (CT) missions, This information can be combined with However, NSA CT organizations do not share a common definition of what constitutes contributing to inconsistent practices and affecting mission performance.

(b) (1)
(b) (3)-P.L. 86-36

(U) Significant Recommendations Outstanding in Previous Semi-annual Reports

(U) **Review of Data Sharing with Third-Party Partners**

(U//~~FOUO~~) NSA's third-party partners are nations other than Australia, Canada, New Zealand, and the United Kingdom with which the U.S. government has national Signals Intelligence (SIGINT) arrangements. The purpose of the review was to determine whether policies and procedures are in place to ensure compliance with authorities for sharing [redacted] with third-party partners. [redacted]

(U//~~FOUO~~) **Finding** Updated policies and process improvements are needed. Documentation for [redacted] disseminated to third-party partners is not centrally maintained. Limited documentation is scattered across many locations throughout the SIGINT Directorate (SID) and the Foreign Affairs Directorate (FAD). Documentation in FAD's Foreign Affairs Knowledge System is not current or easily retrievable.

(U//~~FOUO~~) **Recommendation 1a** FAD should establish a repository for documenting [redacted] shared with third-party partners, and it should update existing documentation. **UPDATE:** FAD has established a repository but has not updated documentation.

~~(C//REL TO USA, FVEY)~~ **Finding** Although SID's Analysis and Production Directorate (S2) developed a process in February 2007 to sample [redacted] disseminated to third-party partners, the process is not well understood, and it has never been reviewed. Quarterly guidance to the S2 workforce on how to sample [redacted] disseminated to partners is unclear, and, as a result, [redacted] is inconsistent.

(U//~~FOUO~~) **Recommendation 2a** SID should revise its oversight process for disseminating [redacted] to partners, including sampling procedures, and inform the workforce of the revised process. SID should also publish an approval authority matrix for third-party activity and formal training on third-party partnerships and provide it to NSA personnel.

(U//~~FOUO~~) **Finding** SID lacks a standard process for [redacted]

(U//~~FOUO~~) **Recommendation 2b and 2c** SID should establish a standard process [redacted]

(b) (1)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) **Special Study of** [redacted]

(U//~~FOUO~~) After the 11 September 2001 terrorist attacks on the United States, NSA established a [redacted] Since then, [redacted] has undergone several reorganizations; most recently, [redacted] became an element of the SIGINT Development Strategy and Governance organization.

(U//~~FOUO~~) **Finding** [redacted] lacks essential mission documentation and standards for NSA Headquarters and the Extended Enterprise.

~~(C//REL TO USA, FVEY)~~ **Recommendation 1b** [redacted] should develop a Mission and Functions Statement, Strategic Plan, and implementing instructions, reflecting the evolving mission of [redacted]

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

[redacted] external agencies. The documents should clearly define internal management controls in standard operating procedures, system configuration management, and budget documentation.

(U//~~FOUO~~) **Finding** [redacted] has no Intelligence Oversight program.

(U//~~FOUO~~) **Recommendation 9a.** The [redacted] should establish an Intelligence Oversight program in accordance with Department of Defense regulations and NSA policies.

(U) Ongoing Special Studies

(~~TS//SI//NF~~) **Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records**

(~~TS//SI//NF~~) The objective of this study is to determine whether controls to ensure NSA compliance with the key terms of the Foreign Intelligence Surveillance Court Order regarding business records are operating as intended.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) **Special Study on Non-traditional Dissemination Methods**

(U//~~FOUO~~) The objective of this study is to evaluate the use of non-traditional dissemination methods for compliance with policies and procedures.

(~~TS//SI//NF~~) **Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Pen Register and Trap and Trace Devices**

(~~TS//SI//NF~~) The audit objective is to determine whether the controls tested as part of a 2010 yearlong review of NSA compliance with seven provisions of the Business Records Order were adequate to provide reasonable assurance of compliance with similar provisions of the Pen Register and Trap and Trace Order.

(U//~~FOUO~~) **Assessment of Management Controls to Implement the FISA Amendments Act of 2008**

(U//~~FOUO~~) The objective of this study is to determine whether NSA controls are adequate to provide reasonable assurance that NSA complies with the terms of the Foreign Intelligence Surveillance Act Amendments Act.

(U//~~FOUO~~) **Special Study of Computer Network Exploitation** [redacted]

(U//~~FOUO~~) The objective of this study is to evaluate [redacted] Foreign Intelligence Surveillance Act operations for compliance with national and NSA policies and procedures.

(~~TS//SI//NF~~) **Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records Retention**

(~~TS//SI//NF~~) The objective of this study is to determine whether NSA controls are adequate to provide reasonable assurance that NSA complies with the terms of the Foreign Intelligence Surveillance Court Order for business records retention.

(U) This page intentionally left blank.

(U) INVESTIGATIONS

(U) Summary of Prosecutions

(U) **Convictions**

- (U) An Agency employee pled guilty in December 2010 to accepting more than $110,000 in bribes from a contractor as part of a scheme to defraud NSA. Sentencing is scheduled for June 2011 in the U.S. District Court in Baltimore, MD.

- (U) A contractor pled guilty in December 2010 to making unlawful payments to a government official as part of a scheme to defraud NSA. On 12 April 2011, the contractor was sentenced in the U.S. District Court in Baltimore, MD, to one year and one day incarceration and three years of supervised release, the first six months of which will be served in home detention.

- (U) A contractor pled guilty in December 2010 to making unlawful payments to a government official as part of a scheme to defraud NSA. Sentencing is scheduled for June 2011 in the U.S. District Court in Baltimore, MD.

(U) Referrals

(U) Three contract labor mischarging investigations are being considered for prosecution. The potential dollar loss exceeds $90,000.

(U) OIG Hotline Action

(U//~~FOUO~~) As the result of an OIG hotline complaint from a member of the public (via unclassified Internet website), an Internet service provider was asked to remove the NSA logo from the profile of a blogger, who was not affiliated with NSA. The Internet service provider complied in March 2011.

(U) This page intentionally left blank.

(U) INDEX OF REPORTING REQUIREMENTS

(U)

IG Act	Reporting Requirement	Page
§5(a)(1)	Significant problems, abuses, and deficiencies	3, 8, 11
§5(a)(2)	Recommendations for corrective action	3, 8, 11
§5(a)(3)	Previously reported significant recommendations not yet completed	3-4, 8-9, 12-13
§5(a)(4)	Matters referred to prosecutive authorities	15
§5(a)(5)	Information or assistance refused	N/A
§5(a)(6)	List of audit, inspection, and evaluation reports	19-20
§5(a)(7)	Summary of significant reports	3, 8, 11
§5(a)(8)	Audit reports with questioned costs	21
§5(a)(9)	Audit reports with funds that could be put to better use	23
§5(a)(10)	Summary of reports for which no management decision was made	N/A
§5(a)(11)	Significant revised management decisions	N/A
§5(a)(12)	Management decision disagreements	N/A

(U)

(U) This page intentionally left blank.

(U) APPENDIX A

(U) AUDITS, INSPECTIONS, AND SPECIAL STUDIES COMPLETED IN THE REPORTING PERIOD

(U) Audits

(U) **Financial Management**

- (U) Audit of Educational Assistance and Recruitment Programs

(U) **Federal Compliance**

- (U) Audit on the FISA Amendments Act §702 Detasking Requirements
- (~~TS//SI//NF~~) Audit of NSA Controls to Comply with the Foreign Intelligence Surveillance Court Order Regarding Business Records – December 2010

(U) **Information Technology**

- (U) Audit of Firewall Management for CES and [redacted] (b)(3)-P.L. 86-36
- (U) Audit Report of NSA/CSS Enterprise Solution and Baseline Exception Request Processes

(U) **Operations**

- (U//~~FOUO~~) Audit of the Nuclear Weapons Personnel Reliability Program

(U) **Business Practices**

- (U) Audit of Market Research and Competition
- (U) Audit of the Power, Space, and Cooling Triage Process for the Extended Enterprise

(U) Inspections

(U) **Joint Inspections**

- (U) Joint Inspection of Alaska Mission Operations Center
- (U) Joint Inspection of Menwith Hill Station
- (U//~~FOUO~~) Joint Inspection of U.S. Central Command

(U) **Field Inspections**

- (U) Field Inspection of Cryptologic Services Group–Marine Corps Intelligence Agency

(U) Special Studies

(U) **Operations**

- (U//~~FOUO~~) Special Study of SIGINT Support to [redacted] (b)(3)-P.L. 86-36

(U) **Federal Compliance**

- (U//~~FOUO~~) Review of Foreign Intelligence Surveillance Court (FISC) Rule 13(a) and 13(b) Filings

(U) APPENDIX B

(U) AUDIT REPORTS WITH QUESTIONED COSTS

(U)

Report	Number	Questioned Costs	Unsupported Costs
For which no management decision had been made by start of reporting period	0	0	0
Issued during reporting period	2	$49,820,000	$920,000
For which management decision was made during reporting period	2	$49,820,000	$920,000
Costs disallowed	1	$920,000	$920,000
Costs not disallowed	0	0	0
For which no management decision was made by end of reporting period	1	$48,900,000	0
(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.			

(U)

(U) This page intentionally left blank.

(U) APPENDIX C

(U) AUDIT REPORTS OF FUNDS THAT COULD BE PUT TO BETTER USE

(U)

Report	Number	Amount
For which no management decision had been made by start of reporting period	0	0
Issued during reporting period	0	0
For which management decision was made during reporting period	0	0
Value of recommendations agreed to by management	0	0
Value of recommendations not agreed to by management	0	0
For which no management decision was made by end of reporting period	0	0
(U) Because our recommendations typically focus on program effectiveness and efficiency and strengthening internal controls, the monetary value of implementing audit recommendations often is not readily quantifiable.		

(U)

(U) This page intentionally left blank.